

HOUSE COMMERCE AND ECONOMIC DEVELOPMENT
COMMITTEE SUBSTITUTE FOR
HOUSE BILL 410

57TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2025

AN ACT

RELATING TO DATA; ENACTING THE CONSUMER INFORMATION AND DATA
PROTECTION ACT; PROVIDING PROCESSES FOR THE COLLECTION AND
PROTECTION OF DATA; PROVIDING DUTIES; PROVIDING EXCEPTIONS;
PROVIDING INVESTIGATIVE AUTHORITY; PROVIDING CIVIL PENALTIES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

SECTION 1. ~~[NEW MATERIAL]~~ SHORT TITLE.--This act may be
cited as the "Consumer Information and Data Protection Act".

SECTION 2. ~~[NEW MATERIAL]~~ DEFINITIONS.--As used in the
Consumer Information and Data Protection Act:

A. "affiliate" means a legal entity that shares
common branding with another legal entity or controls, is
controlled by or is under common control with another legal
entity. For the purposes of this subsection, "control" and
"controlled" mean:

.230941.5ms

underscored material = new
[bracketed material] = delete

1 (1) ownership of, or the power to vote, more
2 than fifty percent of the outstanding shares of any class of
3 voting security of a company;

4 (2) control in any manner over the election of
5 a majority of the directors or of individuals exercising
6 similar functions; or

7 (3) the power to exercise controlling
8 influence over the management of a company;

9 B. "artificial intelligence" means an engineered or
10 machine-based system that varies in its level of autonomy and
11 that can, for explicit or implicit objectives, infer from the
12 input it receives how to generate outputs that can influence
13 physical or virtual environments;

14 C. "authenticate" means to use reasonable means to
15 determine that a request to exercise any of the rights afforded
16 under Section 3 of the Consumer Information and Data Protection
17 Act is being made by, or on behalf of, the consumer who is
18 entitled to exercise such consumer rights with respect to the
19 personal data at issue;

20 D. "biometric data" means data generated by
21 automatic measurements of an individual's biological
22 characteristics, such as a fingerprint, a voiceprint, eye
23 retinas, irises or other unique biological patterns or
24 characteristics that are used to identify a specific
25 individual. "Biometric data" does not include:

.230941.5ms

- 1 (1) a digital or physical photograph;
2 (2) an audio or video recording; or
3 (3) any data generated from a digital or
4 physical photograph, or an audio or video recording, unless
5 such data is generated to identify a specific individual;

6 E. "business associate" has the same meaning as
7 provided in HIPAA;

8 F. "child" means a person under the age of
9 thirteen;

10 G. "cloud computing services" means services that
11 allow access to a scalable and elastic pool of shareable
12 computing resources. Those computing resources include
13 resources such as networks, servers or other infrastructure,
14 storage, applications and services;

15 H. "consent" means a clear affirmative act
16 signifying a consumer's freely given, specific, informed and
17 unambiguous agreement to allow the processing of personal data
18 relating to the consumer. "Consent" may include a written
19 statement, including by electronic means, or any other
20 unambiguous affirmative action. "Consent" does not include:

21 (1) acceptance of a general or broad terms of
22 use or similar document that contains descriptions of personal
23 data processing along with other, unrelated information;

24 (2) hovering over, muting, pausing or closing
25 a given piece of content; or

.230941.5ms

1 (3) agreement obtained through the use of dark
2 patterns;

3 I. "consumer" means an individual who is a resident
4 of this state. "Consumer" does not include an individual
5 acting in a commercial or employment context or as an employee,
6 owner, director, officer or contractor of a company,
7 partnership, sole proprietorship, nonprofit or government
8 agency whose communications or transactions with the controller
9 occur solely within the context of that individual's role with
10 the company, partnership, sole proprietorship, nonprofit or
11 government agency;

12 J. "consumer health data" means any personal data
13 that a controller uses to identify a consumer's physical or
14 mental health condition or diagnosis and includes, but is not
15 limited to, gender-affirming health data and reproductive or
16 sexual health data;

17 K. "controller" means a person who, alone or
18 jointly with others, determines the purpose and means of
19 processing personal data;

20 L. "covered entity" has the same meaning as
21 provided in HIPAA;

22 M. "covered resident" means a natural person who
23 lives in or is domiciled in New Mexico;

24 N. "dark pattern" means a user interface designed
25 or manipulated with the substantial effect of subverting or

1 impairing user autonomy, decision making or choice and includes
 2 any practice the federal trade commission refers to as a "dark
 3 pattern";

4 O. "decisions that produce legal or similarly
 5 significant effects concerning the consumer" means decisions
 6 made by the controller that result in the provision or denial
 7 by the controller of financial or lending services, housing,
 8 insurance, education enrollment or opportunity, criminal
 9 justice, employment opportunities, health care services or
 10 access to essential goods or services;

11 P. "de-identified data" means data that cannot
 12 reasonably be used to infer information about, or otherwise be
 13 linked to, an identified or identifiable individual, or a
 14 device linked to such individual, if the controller that
 15 possesses such data:

16 (1) takes reasonable measures to ensure that
 17 such data cannot be associated with an individual;

18 (2) publicly commits to process such data only
 19 in a de-identified fashion and not attempt to re-identify such
 20 data; and

21 (3) contractually obligates any recipients of
 22 such data to satisfy the criteria set forth in Paragraphs (1)
 23 and (2) of this subsection;

24 Q. "geofence" means any technology that uses global
 25 positioning coordinates, cell tower connectivity, cellular

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 data, radio frequency identification, wireless fidelity
2 technology data or any other form of location detection, or any
3 combination of such coordinates, connectivity, data,
4 identification or other form of location detection, to
5 establish a virtual boundary;

6 R. "heightened risk of harm to minors" means
7 processing minors' personal data in a manner that presents any
8 reasonably foreseeable risk of:

9 (1) any unfair or deceptive treatment of, or
10 any unlawful disparate impact on, minors;

11 (2) any financial, physical or reputational
12 injury to minors; or

13 (3) any physical or other intrusion upon the
14 solitude or seclusion, or the private affairs or concerns, of
15 minors, if the intrusion would be offensive to a reasonable
16 person;

17 S. "HIPAA" means the federal Health Insurance
18 Portability and Accountability Act of 1996, 42 USC 1320d et
19 seq.;

20 T. "identified or identifiable individual" means an
21 individual who can be readily identified, directly or
22 indirectly;

23 U. "institution of higher education" means any
24 individual who, or school, board, association, limited
25 liability company or corporation that, is licensed or

1 accredited to offer one or more programs of higher learning
 2 leading to one or more degrees;

3 V. "mental health facility" means any health care
 4 facility in which at least seventy percent of the health care
 5 services provided in such facility are mental health services;

6 W. "nonprofit organization" means any organization
 7 that is exempt from taxation under Section 501(c)(3),
 8 501(c)(4), 501(c)(6) or 501(c)(12) of the Internal Revenue Code
 9 of 1986, or any subsequent corresponding Internal Revenue Code
 10 of the United States, as amended from time to time;

11 X. "online service, product or feature" means any
 12 service, product or feature that is provided online. "Online
 13 service, product or feature" does not include any:

14 (1) telecommunications service, as defined in
 15 47 USC I 53;

16 (2) broadband internet access service, as
 17 defined in 47 CFR 54.400; or

18 (3) delivery or use of a physical product;

19 Y. "person" means an individual, association,
 20 company, limited liability company, corporation, partnership,
 21 sole proprietorship, trust or other legal entity;

22 Z. "personal data" means any information that is
 23 linked or reasonably linkable to an identified or identifiable
 24 individual. "Personal data" does not include de-identified
 25 data or publicly available information;

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 AA. "precise geolocation data" means information
2 derived from technology, including global positioning system
3 level latitude and longitude coordinates or other mechanisms,
4 that directly identifies the specific location of an individual
5 with precision and accuracy within a radius of one thousand
6 seven hundred fifty feet. "Precise geolocation data" does not
7 include the content of communications or any data generated by
8 or connected to advanced utility metering infrastructure
9 systems or equipment for use by a utility;

10 BB. "process" means any operation or set of
11 operations performed, whether by manual or automated means, on
12 personal data or on sets of personal data, such as the
13 collection, use, storage, disclosure, analysis, deletion or
14 modification of personal data;

15 CC. "processor" means a person who processes
16 personal data on behalf of a controller;

17 DD. "profiling" means any form of automated
18 processing performed on personal data to evaluate, analyze or
19 predict personal aspects related to an identified or
20 identifiable individual's economic situation, health, personal
21 preferences, interests, reliability, behavior, location or
22 movements;

23 EE. "protected health information" has the same
24 meaning as provided in HIPAA;

25 FF. "pseudonymous data" means personal data that

1 cannot be attributed to a specific individual without the use
 2 of additional information; provided that such additional
 3 information is kept separately and is subject to appropriate
 4 technical and organizational measures to ensure that the
 5 personal data is not attributed to an identified or
 6 identifiable individual;

7 GG. "publicly available information" means
 8 information that:

9 (1) is lawfully made available through
 10 federal, state or local government records; and

11 (2) a person has a reasonable basis to believe
 12 a consumer has lawfully made available to the general public;

13 HH. "reproductive or sexual health care" means any
 14 health care-related services or products rendered or provided
 15 concerning a consumer's reproductive system or sexual well-
 16 being, including any such service or product rendered or
 17 provided concerning:

18 (1) an individual health condition, status,
 19 disease, diagnosis, diagnostic test or treatment;

20 (2) a social, psychological, behavioral or
 21 medical intervention;

22 (3) a surgery or procedure, including an
 23 abortion;

24 (4) a use or purchase of a medication,
 25 including, but not limited to, a medication used or purchased

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 for the purposes of an abortion;

2 (5) a bodily function, vital sign or symptom;

3 (6) a measurement of a bodily function, vital
4 sign or symptom; or

5 (7) an abortion, including medical or
6 nonmedical services, products, diagnostics, counseling or
7 follow-up services for an abortion;

8 II. "reproductive or sexual health facility" means
9 any health care facility in which at least seventy percent of
10 the health care-related services or products rendered or
11 provided in such facility are reproductive or sexual health
12 care;

13 JJ. "sale of personal data" means the exchange of
14 personal data for monetary or other valuable consideration by
15 the controller to a third party. "Sale of personal data" does
16 not include:

17 (1) the disclosure of personal data to a
18 processor that processes the personal data on behalf of the
19 controller;

20 (2) the disclosure of personal data to a third
21 party for purposes of providing a product or service requested
22 by the consumer;

23 (3) the disclosure or transfer of personal
24 data to an affiliate of the controller;

25 (4) the disclosure of personal data where the

1 consumer directs the controller to disclose the personal data
 2 or intentionally uses the controller to interact with a third
 3 party;

4 (5) the disclosure of personal data that the
 5 consumer intentionally made available to the general public via
 6 a channel of mass media and did not restrict to a specific
 7 audience; or

8 (6) the disclosure or transfer of personal
 9 data to a third party as an asset that is part of a merger,
 10 acquisition, bankruptcy or other transaction, or a proposed
 11 merger, acquisition, bankruptcy or other transaction, in which
 12 the third party assumes control of all or part of the
 13 controller's assets;

14 KK. "sensitive data" means personal data that
 15 includes:

16 (1) data revealing racial or ethnic origin,
 17 religious beliefs, mental or physical health condition or
 18 diagnosis, sex life, sexual orientation or citizenship or
 19 immigration status;

20 (2) consumer health data;

21 (3) the processing of genetic or biometric
 22 data for the purpose of uniquely identifying an individual;

23 (4) an individual's social security, driver's
 24 license, state identification card or passport number;

25 (5) an individual's account log-in, financial

1 account, debit card or credit card number in combination with
2 any required security or access code, password or credentials
3 allowing access to an account;

4 (6) personal data collected from a known
5 child;

6 (7) data concerning an individual's status as
7 a victim of crime; or

8 (8) precise geolocation data;

9 LL. "targeted advertising" means displaying
10 advertisements to a consumer where the advertisement is
11 selected based on personal data obtained or inferred from that
12 consumer's activities over time and across nonaffiliated
13 internet websites or online applications to predict such
14 consumer's preferences or interests. "Targeted advertising"
15 does not include:

16 (1) advertisements based on activities within
17 a controller's own internet website or online applications;

18 (2) advertisements based on the context of a
19 consumer's current search query, visit to an internet website
20 or online application;

21 (3) advertisements directed to a consumer in
22 response to the consumer's request for information or feedback;
23 or

24 (4) processing personal data solely to measure
25 or report advertising frequency, performance or reach; and

1 MM. "third party" means a person, such as a public
 2 authority, agency or body, other than the consumer, controller
 3 or processor or an affiliate of the processor or the
 4 controller.

5 SECTION 3. [NEW MATERIAL] SCOPE OF ACT--EXEMPTIONS.--

6 A. The Consumer Information and Data Protection Act
 7 applies to persons that conduct business in this state and
 8 persons that produce products or services that are targeted to
 9 residents of this state and that during the preceding calendar
 10 year did any of the following:

11 (1) controlled or processed the personal data
 12 of at least thirty-five thousand consumers, excluding personal
 13 data controlled or processed solely for the purpose of
 14 completing a payment transaction; or

15 (2) controlled or processed the personal data
 16 of at least ten thousand consumers and derived more than twenty
 17 percent of its gross revenue from the sale of personal data.

18 B. No person shall:

19 (1) provide any employee or contractor with
 20 access to consumer health data unless the employee or
 21 contractor is subject to a contractual or statutory duty of
 22 confidentiality;

23 (2) provide any processor with access to
 24 consumer health data unless such person and processor comply
 25 with Section 9 of the Consumer Information and Data Protection

1 Act;

2 (3) use a geofence to establish a virtual
3 boundary that is within one thousand seven hundred fifty feet
4 of any mental health facility or reproductive or sexual health
5 facility for the purpose of identifying, tracking, collecting
6 data from or sending any notification to a consumer regarding
7 the consumer's consumer health data; or

8 (4) sell, or offer to sell, consumer health
9 data without first obtaining the consumer's consent.

10 C. The provisions of the Consumer Information and
11 Data Protection Act shall not apply to any:

12 (1) body, authority, board, bureau,
13 commission, district or agency of the state or of any political
14 subdivision of the state;

15 (2) financial institution or data subject to
16 Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C.
17 Section 6801 et seq.);

18 (3) covered entity or business associate
19 governed by the privacy, security and breach notification rules
20 issued by the federal department of health and human services,
21 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and
22 the Health Information Technology for Economic and Clinical
23 Health Act (P.L. 111-5);

24 (4) nonprofit organization; or

25 (5) institution of higher education.

1 D. The following information and data are exempt
2 from the Consumer Information and Data Protection Act:

3 (1) protected health information under HIPAA;
4 (2) patient identifying information for
5 purposes of 42 U.S.C. Section 290dd-2;

6 (3) identifiable private information for
7 purposes of the federal policy for the protection of human
8 subjects under 45 C.F.R. Part 46; identifiable private
9 information that is otherwise information collected as part of
10 human subjects research pursuant to the good clinical practice
11 guidelines issued by the international council for
12 harmonization of technical requirements for pharmaceuticals for
13 human use; the protection of human subjects under 21 C.F.R.
14 Parts 6, 50 and 56; or personal data used or shared in research
15 conducted in accordance with the requirements set forth in the
16 Consumer Information and Data Protection Act or other research
17 conducted in accordance with applicable law;

18 (4) information and documents created for
19 purposes of the federal Health Care Quality Improvement Act of
20 1986 (42 U.S.C. Section 11101 et seq.);

21 (5) patient safety work product for purposes
22 of the federal Patient Safety and Quality Improvement Act of
23 2005 (42 U.S.C. Section 299b-21 et seq.);

24 (6) information derived from any of the health
25 care-related information listed in this subsection that is de-

.230941.5ms

underscored material = new
[bracketed material] = delete

1 identified in accordance with the requirements for de-
2 identification pursuant to HIPAA;

3 (7) information originating from, and
4 intermingled to be indistinguishable with, or information
5 treated in the same manner as information exempt under this
6 subsection that is maintained by a covered entity or business
7 associate as defined by HIPAA or a program or a qualified
8 service organization as defined by 42 U.S.C. Section 290dd-2;

9 (8) information used only for public health
10 activities and purposes as authorized by HIPAA;

11 (9) the collection, maintenance, disclosure,
12 sale, communication or use of any personal information bearing
13 on a consumer's credit worthiness, credit standing, credit
14 capacity, character, general reputation, personal
15 characteristics or mode of living by a consumer reporting
16 agency or furnisher that provides information for use in a
17 consumer report and by a user of a consumer report but only to
18 the extent that such activity is regulated by and authorized
19 under the federal Fair Credit Reporting Act (15 U.S.C. Section
20 1681 et seq.);

21 (10) personal data collected, processed, sold
22 or disclosed in compliance with the federal Driver's Privacy
23 Protection Act of 1994 (18 U.S.C. Section 2721 et seq.);

24 (11) personal data regulated by the federal
25 Family Educational Rights and Privacy Act of 1974 (20 U.S.C.

.230941.5ms

1 Section 1232g et seq.);

2 (12) personal data collected, processed, sold
 3 or disclosed in compliance with the federal Farm Credit Act of
 4 1971 (12 U.S.C. Section 2001 et seq.); and

5 (13) data processed or maintained:

6 (a) in the course of an individual
 7 applying to, employed by or acting as an agent or independent
 8 contractor of a controller, processor or third party, to the
 9 extent that the data is collected and used within the context
 10 of that role;

11 (b) as the emergency contact information
 12 of an individual under the Consumer Information and Data
 13 Protection Act used for emergency contact purposes; or

14 (c) that is necessary to retain to
 15 administer benefits for another individual relating to the
 16 individual under Subparagraph (a) of this paragraph and used
 17 for the purposes of administering those benefits.

18 SECTION 4. [NEW MATERIAL] CONSUMER RIGHTS.--

19 A. A consumer may invoke the consumer rights
 20 authorized pursuant to this section at any time by submitting a
 21 request to a controller specifying the consumer rights the
 22 consumer wishes to invoke. A known child's parent or legal
 23 guardian may invoke such consumer rights on behalf of the child
 24 regarding processing personal data belonging to the known
 25 child. A controller shall comply with an authenticated

1 consumer request to exercise the right:

2 (1) to confirm whether or not a controller is
3 processing the consumer's personal data and to access such
4 personal data;

5 (2) to correct inaccuracies in the consumer's
6 personal data, taking into account the nature of the personal
7 data and the purposes of the processing of the consumer's
8 personal data;

9 (3) to delete personal data provided by or
10 obtained about the consumer;

11 (4) to obtain a copy of the consumer's
12 personal data that the consumer previously provided to the
13 controller in a portable and, to the extent technically
14 feasible, readily usable format that allows the consumer to
15 transmit the data to another controller without hindrance,
16 where the processing is carried out by automated means; and

17 (5) to opt out of the processing of the
18 personal data for purposes of targeted advertising, the sale of
19 personal data or profiling in furtherance of decisions that
20 produce legal or similarly significant effects concerning the
21 consumer.

22 B. A consumer may exercise rights under this
23 section by a secure and reliable means established by the
24 controller and described to the consumer in the controller's
25 privacy notice. In the case of processing personal data of a

.230941.5ms

1 known child, the parent or legal guardian may exercise such
 2 consumer rights on the child's behalf. In the case of
 3 processing personal data concerning a consumer subject to a
 4 guardianship, conservatorship or other protective arrangement,
 5 the guardian or the conservator of the consumer may exercise
 6 such rights on the consumer's behalf.

7 C. Except as otherwise provided in the Consumer
 8 Information and Data Protection Act, a controller shall comply
 9 with a request by a consumer to exercise the consumer rights
 10 authorized pursuant to Subsection A of this section as follows:

11 (1) a controller shall respond to the consumer
 12 without undue delay, but in all cases within forty-five days of
 13 receipt of the request submitted pursuant to the methods
 14 described in Subsection A of this section. The response period
 15 may be extended once by forty-five additional days when
 16 reasonably necessary, taking into account the complexity and
 17 number of the consumer's requests, so long as the controller
 18 informs the consumer of any such extension within the initial
 19 forty-five-day response period, together with the reason for
 20 the extension;

21 (2) if a controller declines to take action
 22 regarding the consumer's request, the controller shall inform
 23 the consumer without undue delay, but in all cases and at the
 24 latest within forty-five days of receipt of the request, of the
 25 justification for declining to take action and instructions for

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 how to appeal the decision pursuant to Subsection D of this
2 section;

3 (3) information provided in response to a
4 consumer request shall be provided by a controller free of
5 charge, up to twice annually per consumer. If requests from a
6 consumer are manifestly unfounded, excessive or repetitive, the
7 controller may charge the consumer a reasonable fee to cover
8 the administrative costs of complying with the request or
9 decline to act on the request. The controller bears the burden
10 of demonstrating the manifestly unfounded, excessive or
11 repetitive nature of the request;

12 (4) if a controller is unable to authenticate
13 the request using commercially reasonable efforts, the
14 controller shall not be required to comply with a request to
15 initiate an action under Subsection A of this section and may
16 request that the consumer provide additional information
17 reasonably necessary to authenticate the consumer and the
18 consumer's request;

19 (5) a controller that has obtained personal
20 data about a consumer from a source other than the consumer
21 shall be deemed in compliance with a consumer's request to
22 delete such data pursuant to Paragraph (2) of Subsection A of
23 this section by either:

24 (a) retaining a record of the deletion
25 request and the minimum data necessary for the purpose of

1 ensuring the consumer's personal data remains deleted from the
 2 business's records and not using such retained data for any
 3 other purpose pursuant to the provisions of the Consumer
 4 Information and Data Protection Act; or

5 (b) opting the consumer out of the
 6 processing of such personal data for any purpose except for
 7 those exempted pursuant to the provisions of the Consumer
 8 Information and Data Protection Act; and

9 (6) providing an effective mechanism for a
 10 consumer to revoke the consumer's consent under this section
 11 that is at least as easy as the mechanism by which the consumer
 12 provided the consumer's consent and, upon revocation of such
 13 consent, cease to process the data as soon as practicable, but
 14 not later than fifteen days after the receipt of such request.

15 D. A controller shall establish a process for a
 16 consumer to appeal the controller's refusal to take action on a
 17 request within a reasonable period of time after the consumer's
 18 receipt of the decision pursuant to Paragraph (2) of Subsection
 19 C of this section. The appeal process shall be conspicuously
 20 available and similar to the process for submitting requests to
 21 initiate action pursuant to Subsection A of this section.

22 Within sixty days of receipt of an appeal, a controller shall
 23 inform the consumer in writing of any action taken or not taken
 24 in response to the appeal, including a written explanation of
 25 the reasons for the decisions. If the appeal is denied, the

.230941.5ms

1 controller shall also provide the consumer with an online
2 mechanism, if available, or other method through which the
3 consumer may contact the attorney general to submit a
4 complaint.

5 SECTION 5. [NEW MATERIAL] AUTHORIZED AGENTS AND CONSUMER
6 OPT-OUT.--A consumer may designate another person to serve as
7 the consumer's authorized agent, and act on such consumer's
8 behalf, to opt out of the processing of such consumer's
9 personal data for one or more of the purposes specified in
10 Section 4 of the Consumer Information and Data Protection Act.
11 The consumer may designate such authorized agent by way of,
12 among other things, a technology, including, but not limited
13 to, an internet link or a browser setting, browser extension or
14 global device setting, indicating such consumer's intent to opt
15 out of such processing. A controller shall comply with an
16 opt-out request received from an authorized agent if the
17 controller is able to verify, with commercially reasonable
18 effort, the identity of the consumer and the authorized agent's
19 authority to act on such consumer's behalf.

20 SECTION 6. [NEW MATERIAL] DATA CONTROLLER
21 RESPONSIBILITIES--TRANSPARENCY.--

22 A. A controller shall:

23 (1) limit the collection of personal data to
24 what is adequate, relevant and reasonably necessary in relation
25 to the purposes for which such data is processed, as disclosed

1 to the consumer;

2 (2) except as otherwise provided in the
 3 Consumer Information and Data Protection Act, not process
 4 personal data for purposes that are neither reasonably
 5 necessary to nor compatible with the disclosed purposes for
 6 which such personal data is processed, as disclosed to the
 7 consumer, unless the controller obtains the consumer's consent;

8 (3) establish, implement and maintain
 9 reasonable administrative, technical and physical data security
 10 practices to protect the confidentiality, integrity and
 11 accessibility of personal data. Data security practices shall
 12 be appropriate to the volume and nature of the personal data at
 13 issue;

14 (4) not process personal data in violation of
 15 state and federal laws that prohibit unlawful discrimination
 16 against consumers. A controller shall not discriminate against
 17 a consumer for exercising any of the consumer rights contained
 18 in the Consumer Information and Data Protection Act, including
 19 denying goods or services, charging different prices or rates
 20 for goods or services or providing a different level of quality
 21 of goods and services to the consumer. However, nothing in
 22 this subsection shall be construed to require a controller to
 23 provide a product or service that requires the personal data of
 24 a consumer that the controller does not collect or maintain or
 25 to prohibit a controller from offering a different price, rate,

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 level, quality or selection of goods or services to a consumer,
2 including offering goods or services for no fee, if the
3 consumer has exercised the consumer's right to opt out pursuant
4 to Section 4 of the Consumer Information and Data Protection
5 Act or the offer is related to a consumer's voluntary
6 participation in a bona fide loyalty, rewards, premium
7 features, discounts or club card program; and

8 (5) not process sensitive data concerning a
9 consumer without obtaining the consumer's consent or, in the
10 case of the processing of sensitive data concerning a known
11 child, without processing such data in accordance with the
12 federal Children's Online Privacy Protection Act of 1998 (15
13 U.S.C. Section 6501 et seq.).

14 B. Any provision of a contract or agreement of any
15 kind that purports to waive or limit in any way consumer rights
16 pursuant to the Consumer Information and Data Protection Act
17 shall be deemed contrary to public policy and shall be void and
18 unenforceable.

19 C. A controller shall provide consumers with a
20 reasonably accessible, clear and meaningful privacy notice that
21 includes:

22 (1) the categories of personal data processed
23 by the controller;

24 (2) the purpose for processing personal data;

25 (3) how consumers may exercise their consumer

1 rights, including how a consumer may appeal a controller's
 2 decision with regard to the consumer's request;

3 (4) the categories of personal data that the
 4 controller shares with third parties, if any;

5 (5) the categories of third parties, if any,
 6 with which the controller shares personal data; and

7 (6) an active electronic mail address or other
 8 online mechanism that the consumer may use to contact the
 9 controller.

10 D. If a controller sells personal data to third
 11 parties or processes personal data for targeted advertising,
 12 the controller shall clearly and conspicuously disclose such
 13 processing, as well as the manner in which a consumer may
 14 exercise the right to opt out of such processing.

15 E. A controller shall establish, and shall describe
 16 in a privacy notice, one or more secure and reliable means for
 17 consumers to submit a request to exercise their consumer rights
 18 under the Consumer Information and Data Protection Act. Such
 19 means shall take into account the ways in which consumers
 20 normally interact with the controller, the need for secure and
 21 reliable communication of such requests and the ability of the
 22 controller to authenticate the identity of the consumer making
 23 the request. Controllers shall not require a consumer to
 24 create a new account in order to exercise consumer rights
 25 pursuant to Section 4 of the Consumer Information and Data

.230941.5ms

1 Protection Act but may require a consumer to use an existing
2 account.

3 F. Subject to the consent requirement established
4 by Section 4 of the Consumer Information and Data Protection
5 Act, no controller shall process any personal data collected
6 from a known child:

7 (1) for the purposes of targeted advertising,
8 the sale of such personal data or profiling in furtherance of
9 decisions that produce legal or similarly significant effects
10 concerning a consumer;

11 (2) unless such processing is reasonably
12 necessary to provide the online service, product or feature;

13 (3) for any processing purpose other than the
14 processing purpose that the controller disclosed at the time
15 such controller collected such personal data or that is
16 reasonably necessary for and compatible with such disclosed
17 purpose; or

18 (4) for longer than is reasonably necessary to
19 provide the online service, product or feature.

20 G. Subject to the consent requirement established
21 by Section 4 of the Consumer Information and Data Protection
22 Act, no controller shall collect precise geolocation data from
23 a known child unless:

24 (1) such precise geolocation data is
25 reasonably necessary for the controller to provide an online

1 service, product or feature and, if such data is necessary to
 2 provide such online service, product or feature, such
 3 controller shall only collect such data for the time necessary
 4 to provide such online service, product or feature; and

5 (2) the controller provides to the known child
 6 a signal indicating that such controller is collecting such
 7 precise geolocation data, which signal shall be available to
 8 such known child for the entire duration of such collection.

9 H. No controller shall engage in the activities
 10 described in Subsections F and G of Section 4 of the Consumer
 11 Information and Data Protection Act unless the controller
 12 obtains consent from the child's parent or legal guardian in
 13 accordance with the federal Children's Online Privacy
 14 Protection Act of 1998 (15 U.S.C. Section 6501 et seq.).

15 SECTION 7. [NEW MATERIAL] DATA CONTROLLER
 16 RESPONSIBILITIES--ONLINE SERVICE, PRODUCT OR FEATURE.--

17 A. Each controller that offers an online service,
 18 product or feature to consumers who are minors younger than the
 19 age of eighteen, whom the controller has actual knowledge or
 20 willfully disregards that they are minors younger than the age
 21 of eighteen, shall use reasonable care to avoid any heightened
 22 risk of harm to such minors caused by the online service,
 23 product or feature.

24 B. Subject to the consent requirement established
 25 in Subsection D of this section, no controller that offers any

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 online service, product or feature to consumers whom the
2 controller has actual knowledge or willfully disregards are
3 minors younger than the age of eighteen shall:

4 (1) process personal data of any minor younger
5 than the age of eighteen for the purposes of:

- 6 (a) targeted advertising;
7 (b) any sale of personal data; or
8 (c) profiling in furtherance of any
9 fully automated decision made by such controller that produces
10 any legal or similarly significant effect concerning the
11 provision or denial by such controller of any financial or
12 lending services, housing, insurance, education enrollment or
13 opportunity, criminal justice, employment opportunity, health
14 care services or access to essential goods or services, unless
15 such processing is reasonably necessary to provide the online
16 service, product or feature, or for any processing purpose
17 other than the processing purpose that the controller disclosed
18 at the time the controller collected the personal data, or that
19 is reasonably necessary for, and compatible with, the
20 processing purpose described in this subsection, or for longer
21 than is reasonably necessary to provide the online service,
22 product or feature; or

23 (2) use any system design feature to
24 significantly increase, sustain or extend any minor younger
25 than the age of eighteen's use of such online service, product

1 or feature. The provisions of this subsection shall not apply
 2 to any service or application that is used by and under the
 3 direction of an educational entity, including a learning
 4 management system or a student engagement program.

5 C. Subject to the consent requirement established
 6 in Subsection D of this section, no controller that offers an
 7 online service, product or feature to consumers whom the
 8 controller has actual knowledge, or willfully disregards, are
 9 minors younger than the age of eighteen shall collect the
 10 minor's precise geolocation data unless:

11 (1) precise geolocation data is reasonably
 12 necessary for the controller to provide the online service,
 13 product or feature and, if the data are necessary to provide
 14 the online service, product or feature, the controller may only
 15 collect the data for the time necessary to provide the online
 16 service, product or feature; and

17 (2) the controller provides to the minor a
 18 signal indicating that the controller is collecting the precise
 19 geolocation data, which signal shall be available to the minor
 20 for the entire duration of such collection.

21 D. No controller that offers any online service,
 22 product or feature to consumers whom the controller has actual
 23 knowledge or willfully disregards are minors younger than the
 24 age of eighteen shall engage in the activities described in
 25 Subsections B and C of this section unless the controller

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 obtains the consent of the minor younger than the age of
2 eighteen, or, if the minor is younger than thirteen years of
3 age, the consent of the minor's parent or legal guardian. A
4 controller that complies with the verifiable parental consent
5 requirements established in the federal Children's Online
6 Privacy Protection Act of 1998, 15 USC 6501 et seq., and the
7 regulations, rules, guidance and exemptions adopted pursuant to
8 that act, as that act and the regulations, rules, guidance and
9 exemptions may be amended from time to time, shall be deemed to
10 have satisfied any requirement to obtain parental consent under
11 this subsection.

12 E. No controller that offers any online service,
13 product or feature to consumers whom the controller has actual
14 knowledge, or willfully disregards, are minors younger than the
15 age of eighteen shall:

16 (1) provide any consent mechanism that is
17 designed to substantially subvert or impair, or is manipulated
18 with the effect of substantially subverting or impairing, user
19 autonomy, decision-making or choice; or

20 (2) except as provided in Subsection F of this
21 section, offer any direct messaging apparatus for use by minors
22 without providing readily accessible and easy-to-use safeguards
23 to limit the ability of adults to send unsolicited
24 communications to minors with whom they are not connected.

25 F. The provisions of Paragraph (2) of Subsection B

1 of this section shall not apply to services when the
2 predominant or exclusive function is:

3 (1) electronic mail; or
4 (2) direct messaging consisting of text,
5 photos or videos that are sent between devices by electronic
6 means, if messages are:

7 (a) shared between the sender and the
8 recipient;

9 (b) only visible to the sender and the
10 recipient; and

11 (c) not posted publicly.

12 SECTION 8. [NEW MATERIAL] DATA CONTROLLER

13 RESPONSIBILITIES--ONLINE SERVICE, PRODUCT OR FEATURE--DATA
14 PROTECTION ASSESSMENTS, REVIEW AND RECORD KEEPING.--

15 A. Each controller that, on or after one year after
16 the effective date of the Consumer Information and Data
17 Protection Act, offers any online service, product or feature
18 to consumers whom the controller has actual knowledge, or
19 willfully disregards, are minors younger than the age of
20 eighteen shall conduct a data protection assessment for such
21 online service, product or feature:

22 (1) in a manner that is consistent with the
23 requirements established in Section 7 of that act; and

24 (2) that addresses:

25 (a) the purpose of the online service,

.230941.5ms

1 product or feature;

2 (b) the categories of minors' personal
3 data that the online service, product or feature processes;

4 (c) the purposes for which the
5 controller processes minors' personal data with respect to the
6 online service, product or feature; and

7 (d) any heightened risk of harm to
8 minors that is a reasonably foreseeable result of offering the
9 online service, product or feature to minors.

10 B. Each controller that conducts a data protection
11 assessment pursuant to Subsection A of this section shall:

12 (1) review the data protection assessment as
13 necessary to account for any material change to the processing
14 operations of the online service, product or feature that is
15 the subject of the data protection assessment; and

16 (2) maintain documentation concerning the data
17 protection assessment for the longer of:

18 (a) the three-year period beginning on
19 the date on which the processing operations cease; or

20 (b) as long as the controller offers the
21 online service, product or feature.

22 C. A single data protection assessment may address
23 a comparable set of processing operations that include similar
24 activities.

25 D. If a controller conducts a data protection

1 assessment for the purpose of complying with another applicable
 2 law or regulation, the data protection assessment shall be
 3 deemed to satisfy the requirements established in this section
 4 if the data protection assessment is reasonably similar in
 5 scope and effect to the data protection assessment that would
 6 otherwise be conducted pursuant to this section.

7 E. If a controller conducts a data protection
 8 assessment pursuant to Subsection A of this section and
 9 determines that the online service, product or feature that is
 10 the subject of the assessment poses a heightened risk of harm
 11 to minors, the controller shall establish and implement a plan
 12 to mitigate or eliminate the risk.

13 F. Data protection assessments shall be
 14 confidential and shall be exempt from disclosure under the
 15 Inspection of Public Records Act. To the extent that any
 16 information contained in a data protection assessment disclosed
 17 to the attorney general includes information subject to
 18 attorney-client privilege or work product protection, the
 19 disclosure shall not constitute a waiver of the privilege or
 20 protection.

21 SECTION 9. [NEW MATERIAL] RESPONSIBILITIES OF CONTROLLER
 22 AND PROCESSOR.--

23 A. A processor shall adhere to the instructions of
 24 a controller and shall assist the controller in meeting its
 25 obligations under the Consumer Information and Data Protection

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 Act. Such assistance shall include:

2 (1) taking into account the nature of
3 processing and the information available to the processor, by
4 appropriate technical and organizational measures, insofar as
5 this is reasonably practicable, to fulfill the controller's
6 obligation to respond to consumer rights requests pursuant to
7 Section 4 of the Consumer Information and Data Protection Act;

8 (2) taking into account the nature of
9 processing and the information available to the processor, by
10 assisting the controller in meeting the controller's
11 obligations in relation to the security of processing the
12 personal data and in relation to the notification of a breach
13 of security of the system of the processor pursuant to the
14 Consumer Information and Data Protection Act in order to meet
15 the controller's obligations; and

16 (3) providing necessary information to enable
17 the controller to conduct and document data protection
18 assessments pursuant to the Consumer Information and Data
19 Protection Act.

20 B. A contract between a controller and a processor
21 shall govern the processor's data processing procedures with
22 respect to processing performed on behalf of the controller.
23 The contract shall be binding and clearly set forth
24 instructions for processing data, the nature and purpose of
25 processing, the type of data subject to processing, the

.230941.5ms

1 duration of processing and the rights and obligations of both
 2 parties. The contract shall also include requirements that the
 3 processor shall:

4 (1) ensure that each person processing
 5 personal data is subject to a duty of confidentiality with
 6 respect to the data;

7 (2) at the controller's direction, delete or
 8 return all personal data to the controller as requested at the
 9 end of the provision of services, unless retention of the
 10 personal data is required by law;

11 (3) upon the reasonable request of the
 12 controller, make available to the controller all information in
 13 its possession necessary to demonstrate the processor's
 14 compliance with the obligations in the Consumer Information and
 15 Data Protection Act;

16 (4) allow, and cooperate with, reasonable
 17 assessments by the controller or the controller's designated
 18 assessor; alternatively, the processor may arrange for a
 19 qualified and independent assessor to conduct an assessment of
 20 the processor's policies and technical and organizational
 21 measures in support of the obligations under the Consumer
 22 Information and Data Protection Act using an appropriate and
 23 accepted control standard or framework and assessment procedure
 24 for such assessments. The processor shall provide a report of
 25 such assessment to the controller upon request; and

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 (5) engage any subcontractor pursuant to a
2 written contract in accordance with this section that requires
3 the subcontractor to meet the obligations of the processor with
4 respect to the personal data.

5 C. Nothing in this section shall be construed to
6 relieve a controller or a processor from the liabilities
7 imposed on it by virtue of its role in the processing
8 relationship as defined by the Consumer Information and Data
9 Protection Act.

10 D. Determining whether a person is acting as a
11 controller or processor with respect to a specific processing
12 of data is a fact-based determination that depends upon the
13 context in which personal data is to be processed. A processor
14 that continues to adhere to a controller's instructions with
15 respect to a specific processing of personal data remains a
16 processor.

17 SECTION 10. [NEW MATERIAL] DATA PROTECTION ASSESSMENTS.--

18 A. A controller shall conduct and document a data
19 protection assessment of each of the following processing
20 activities involving personal data:

21 (1) the processing of personal data for
22 purposes of targeted advertising;

23 (2) the sale of personal data;

24 (3) the processing of personal data for
25 purposes of profiling, where such profiling presents a

1 reasonably foreseeable risk of:

2 (a) unfair or deceptive treatment of, or
 3 unlawful disparate impact on, consumers;

4 (b) financial, physical or reputational
 5 injury to consumers;

6 (c) a physical or other intrusion upon
 7 the solitude or seclusion, or the private affairs or concerns,
 8 of consumers, where such intrusion would be offensive to a
 9 reasonable person; or

10 (d) other substantial injury to
 11 consumers;

12 (4) the processing of sensitive data; and

13 (5) any processing activities involving
 14 personal data that present a heightened risk of harm to
 15 consumers.

16 B. Data protection assessments conducted pursuant
 17 to Subsection A of this section shall identify and weigh the
 18 benefits that may flow, directly and indirectly, from the
 19 processing to the controller, the consumer, other stakeholders
 20 and the public against the potential risks to the rights of the
 21 consumer associated with such processing, as mitigated by
 22 safeguards that can be employed by the controller to reduce
 23 such risks. The use of de-identified data and the reasonable
 24 expectations of consumers, as well as the context of the
 25 processing and the relationship between the controller and the

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 consumer whose personal data will be processed, shall be
2 factored into this assessment by the controller.

3 C. The attorney general may request, pursuant to a
4 civil investigative demand, that a controller disclose any data
5 protection assessment that is relevant to an investigation
6 conducted by the attorney general, and the controller shall
7 make the data protection assessment available to the attorney
8 general. The attorney general may evaluate the data protection
9 assessment for compliance with the responsibilities set forth
10 in Subsection A of this section. Data protection assessments
11 shall be confidential and exempt from public inspection and
12 copying under the Inspection of Public Records Act. The
13 disclosure of a data protection assessment pursuant to a
14 request from the attorney general shall not constitute a waiver
15 of attorney-client privilege or work product protection with
16 respect to the assessment and any information contained in the
17 assessment.

18 D. A single data protection assessment may address
19 a comparable set of processing operations that include similar
20 activities.

21 E. Data protection assessments conducted by a
22 controller for the purpose of compliance with other laws or
23 regulations may comply under this section if the assessments
24 have a reasonably comparable scope and effect.

25 F. Data protection assessment requirements shall

1 apply to processing activities created or generated after the
2 effective date of the Consumer Information and Data Protection
3 Act and are not retroactive.

4 SECTION 11. [NEW MATERIAL] PROCESSING DE-IDENTIFIED
5 DATA.--

6 A. The controller in possession of de-identified
7 data shall:

8 (1) take reasonable measures to ensure that
9 the data cannot be associated with a natural person;

10 (2) publicly commit to maintaining and using
11 de-identified data without attempting to re-identify the data;
12 and

13 (3) contractually obligate any recipients of
14 the de-identified data to comply with all provisions of the
15 Consumer Information and Data Protection Act.

16 B. Nothing in the Consumer Information and Data
17 Protection Act shall be construed to require a controller or
18 processor to re-identify de-identified data or pseudonymous
19 data or maintain data in identifiable form, or collect, obtain,
20 retain or access any data or technology, in order to be capable
21 of associating an authenticated consumer request with personal
22 data.

23 C. Nothing in the Consumer Information and Data
24 Protection Act shall be construed to require a controller or
25 processor to comply with an authenticated consumer rights

.230941.5ms

1 request, pursuant to Section 4 of the Consumer Information and
2 Data Protection Act, if all of the following are true:

3 (1) the controller is not reasonably capable
4 of associating the request with the personal data or it would
5 be unreasonably burdensome for the controller to associate the
6 request with the personal data;

7 (2) the controller does not use the personal
8 data to recognize or respond to the specific consumer who is
9 the subject of the personal data or associate the personal data
10 with other personal data about the same specific consumer; and

11 (3) the controller does not sell the personal
12 data to any third party or otherwise voluntarily disclose the
13 personal data to any third party other than a processor, except
14 as otherwise permitted in this section.

15 D. The consumer rights contained in Section 4 of
16 the Consumer Information and Data Protection Act shall not
17 apply to pseudonymous data in cases where the controller is
18 able to demonstrate any information necessary to identify the
19 consumer is kept separately and is subject to effective
20 technical and organizational controls that prevent the
21 controller from accessing such information.

22 E. A controller that discloses pseudonymous data or
23 de-identified data shall exercise reasonable oversight to
24 monitor compliance with any contractual commitments to which
25 the pseudonymous data or de-identified data is subject and

.230941.5ms

1 shall take appropriate steps to address any breaches of those
 2 contractual commitments.

3 SECTION 12. [NEW MATERIAL] LIMITATIONS.--

4 A. Nothing in the Consumer Information and Data
 5 Protection Act shall be construed to restrict a controller's or
 6 processor's ability to:

7 (1) comply with federal, state or local laws,
 8 rules or regulations;

9 (2) comply with a civil, criminal or
 10 regulatory inquiry, investigation, subpoena or summons by
 11 federal, state, local or other governmental authorities;

12 (3) cooperate with law enforcement agencies
 13 concerning conduct or activity that the controller or processor
 14 reasonably and in good faith believes may violate federal,
 15 state or local laws, rules or regulations;

16 (4) investigate, establish, exercise, prepare
 17 for or defend legal claims;

18 (5) provide a product or service specifically
 19 requested by a consumer, perform a contract to which the
 20 consumer is a party, including fulfilling the terms of a
 21 written warranty, or take steps at the request of the consumer
 22 prior to entering into a contract;

23 (6) take immediate steps to protect an
 24 interest that is essential for the life or physical safety of
 25 the consumer or of another natural person and where the

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 processing cannot be manifestly based on another legal basis;

2 (7) prevent, detect, protect against or
3 respond to security incidents, identity theft, fraud,
4 harassment, malicious or deceptive activities or any illegal
5 activity; preserve the integrity or security of systems; or
6 investigate, report or prosecute those responsible for any such
7 action;

8 (8) engage in public or peer-reviewed
9 scientific or statistical research in the public interest that
10 adheres to all other applicable ethics and privacy laws and is
11 approved, monitored and governed by an institutional review
12 board or similar independent oversight entities that determine:

13 (a) if the deletion of the information
14 is likely to provide substantial benefits that do not
15 exclusively accrue to the controller;

16 (b) the expected benefits of the
17 research outweigh the privacy risks; and

18 (c) if the controller has implemented
19 reasonable safeguards to mitigate privacy risks associated with
20 research, including any risks associated with re-
21 identification; or

22 (9) assist another controller, processor or
23 third party with any of the obligations under this subsection.

24 B. The obligations imposed on controllers or
25 processors under the Consumer Information and Data Protection

1 Act shall not restrict a controller's or processor's ability to
 2 collect, use or retain data to:

- 3 (1) conduct internal research to develop,
 4 improve or repair products, services or technology;
- 5 (2) effectuate a product recall;
- 6 (3) identify and repair technical errors that
 7 impair existing or intended functionality; or
- 8 (4) perform internal operations that are
 9 reasonably aligned with the expectations of the consumer or
 10 reasonably anticipated based on the consumer's existing
 11 relationship with the controller or are otherwise compatible
 12 with processing data in furtherance of the provision of a
 13 product or service specifically requested by a consumer or the
 14 performance of a contract to which the consumer is a party.

15 C. The obligations imposed on controllers or
 16 processors under the Consumer Information and Data Protection
 17 Act shall not apply where compliance by the controller or
 18 processor with that act would violate an evidentiary privilege
 19 under the laws of the state. Nothing in that act shall be
 20 construed to prevent a controller or processor from providing
 21 personal data concerning a consumer to a person covered by an
 22 evidentiary privilege under the laws of the state as part of a
 23 privileged communication.

24 D. A controller or processor that discloses
 25 personal data to a third-party controller or processor, in

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 compliance with the requirements of the Consumer Information
2 and Data Protection Act, is not in violation of that act if the
3 third-party controller or processor that receives and processes
4 such personal data is in violation of that act; provided that,
5 at the time of disclosing the personal data, the disclosing
6 controller or processor did not have actual knowledge that the
7 recipient intended to commit a violation. A third-party
8 controller or processor receiving personal data from a
9 controller or processor in compliance with the requirements of
10 that act is likewise not in violation of that act for the
11 transgressions of the controller or processor from which it
12 receives such personal data.

13 E. Nothing in the Consumer Information and Data
14 Protection Act shall be construed as an obligation imposed on
15 controllers and processors that adversely affects the rights or
16 freedoms of any persons, such as exercising the right of free
17 speech pursuant to the first amendment to the United States
18 constitution, or applies to the processing of personal data by
19 a person in the course of a purely personal or household
20 activity.

21 F. Personal data processed by a controller pursuant
22 to this section shall not be processed for any purpose other
23 than those expressly listed in this section unless otherwise
24 allowed by the Consumer Information and Data Protection Act.
25 Personal data processed by a controller pursuant to this

1 section may be processed to the extent that such processing is:

2 (1) reasonably necessary and proportionate to
 3 the purposes listed in this section; and

4 (2) adequate, relevant and limited to what is
 5 necessary in relation to the specific purposes listed in this
 6 section. Personal data collected, used or retained pursuant to
 7 Subsection B of this section shall, where applicable, take into
 8 account the nature and purpose or purposes of such collection,
 9 use or retention. Such data shall be subject to reasonable
 10 administrative, technical and physical measures to protect the
 11 confidentiality, integrity and accessibility of the personal
 12 data and to reduce reasonably foreseeable risks of harm to
 13 consumers relating to such collection, use or retention of
 14 personal data.

15 G. If a controller processes personal data pursuant
 16 to an exemption in this section, the controller bears the
 17 burden of demonstrating that such processing qualifies for the
 18 exemption and complies with the requirements in Subsection F of
 19 this section.

20 H. Processing personal data for the purposes
 21 expressly identified in Subsection A of this section shall not
 22 solely make an entity a controller with respect to such
 23 processing.

24 SECTION 13. [NEW MATERIAL] DATA IN THE POSSESSION OF
 25 FEDERAL AGENCIES.--

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 A. No person may share, disclose, re-disclose or
2 otherwise disseminate a covered resident's sensitive data in
3 the possession of a federal agency without the consent of the
4 covered resident, except where that disclosure is pursuant to a
5 law lawfully enacted by the United States congress.

6 B. A third party that receives sensitive data from
7 the federal government or its agents, without express
8 authorization by a law enacted by the United States congress
9 permitting such disclosure, upon request by the covered
10 resident or the attorney general shall:

11 (1) delete the information in its possession;
12 and

13 (2) disclose the source from which the
14 information was obtained.

15 C. A person who receives a request or demand for a
16 covered resident's sensitive data in the possession of a
17 federal agency without the consent of the covered resident
18 shall not share, disclose, re-disclose or otherwise disseminate
19 such data without first receiving an order of a court of
20 competent jurisdiction that such disclosure is pursuant to a
21 law enacted by the United States congress.

22 D. The attorney general may enforce the provisions
23 of this section and may intervene as a matter of right in any
24 action seeking a determination as to whether the requested
25 disclosure is pursuant to a law enacted by the United States

1 congress.

2 E. The attorney general may enforce the provisions
 3 of this section and is empowered to issue a civil investigation
 4 demand whenever the attorney general has reasonable cause to
 5 believe that any person has engaged in, is engaging in or is
 6 about to engage in any violation of this section. A person
 7 issued an investigative demand shall produce the material
 8 sought and shall permit it to be copied and inspected by the
 9 attorney general. The demand of the attorney general and any
 10 material produced in response to it shall not be a matter of
 11 public record and shall not be published by the attorney
 12 general except by order of the court.

13 F. Upon reasonable belief that there has been a
 14 violation of this section, the attorney general:

15 (1) may bring an action in the name of the
 16 state to enforce the provisions of this section;

17 (2) may petition the court for injunctive
 18 relief; and

19 (3) shall not be required to post bond when
 20 seeking a temporary or permanent injunction.

21 SECTION 14. [NEW MATERIAL] INVESTIGATIVE AUTHORITY.--
 22 Whenever the attorney general has reasonable cause to believe
 23 that any person has engaged in, is engaging in or is about to
 24 engage in any violation of the Consumer Information and Data
 25 Protection Act, the attorney general is empowered to issue a

underscored material = new
 [bracketed material] = delete

1 civil investigative demand.

2 SECTION 15. [NEW MATERIAL] ENFORCEMENT--CIVIL
3 PENALTIES.--

4 A. The attorney general shall have authority to
5 enforce the provisions of the Consumer Information and Data
6 Protection Act.

7 B. Prior to initiating any action under the
8 Consumer Information and Data Protection Act other than as
9 specified in Section 13 of that act, the attorney general shall
10 provide a controller or processor thirty days' written notice
11 identifying the specific provisions of the Consumer Information
12 and Data Protection Act the attorney general alleges have been
13 or are being violated. If within the thirty-day period the
14 controller or processor cures the noticed violation and
15 provides the attorney general an express written statement that
16 the alleged violations have been cured and that no further
17 violations shall occur, no action shall be initiated against
18 the controller or processor.

19 C. If a controller or processor continues to
20 violate the Consumer Information and Data Protection Act
21 following the cure period in Subsection B of this section or
22 breaches an express written statement provided to the attorney
23 general under that subsection, the attorney general may
24 initiate an action and may seek an injunction to restrain any
25 violations of that act and civil penalties of up to ten

1 thousand dollars (\$10,000) for each violation under that act.

2 D. The attorney general may recover reasonable
 3 attorney fees and costs of investigation and enforcement
 4 whenever a court finds a violation of the Consumer Information
 5 and Data Protection Act.

6 E. Nothing in the Consumer Information and Data
 7 Protection Act shall be construed as providing the basis for,
 8 or be subject to, a private right of action for violations of
 9 that act or under any other law.

10 SECTION 16. [NEW MATERIAL] SEVERABILITY.--

11 A. Every provision, section, subsection, sentence,
 12 clause, phrase or word in the Consumer Information and Data
 13 Protection Act, and every application of the provisions in that
 14 act, are severable from each other.

15 B. If any application of any provision in the
 16 Consumer Information and Data Protection Act to any person,
 17 group of persons or circumstances is found by a court to be
 18 invalid or unconstitutional, the remaining applications of that
 19 provision to all other persons and circumstances shall be
 20 severed and shall not be affected. All constitutionally valid
 21 applications of the Consumer Information and Data
 22 Protection Act shall be severed from any applications that a
 23 court finds to be invalid, leaving the valid applications in
 24 force, because it is the legislature's intent and priority that
 25 the valid applications be allowed to stand alone. Even if a

.230941.5ms

underscored material = new
 [bracketed material] = delete

1 reviewing court finds a provision of the Consumer Information
2 and Data Protection Act to impose an undue burden in a large or
3 substantial fraction of relevant cases, the applications that
4 do not present an undue burden shall be severed from the
5 remaining applications, shall remain in force and shall be
6 treated as if the legislature had enacted a statute limited to
7 the persons, group of persons or circumstances for which the
8 statute's application does not present an undue burden.

9 C. If any court declares or finds a provision of
10 the Consumer Information and Data Protection Act facially
11 unconstitutional, when discrete applications of that provision
12 can be enforced against a person, group of persons or
13 circumstances without violating the United States constitution
14 and the constitution of New Mexico, those applications shall be
15 severed from all remaining applications of the provision, and
16 the provision shall be interpreted as if the legislature had
17 enacted a provision limited to the persons, group of persons or
18 circumstances for which the provision's application will not
19 violate the United States constitution and the constitution of
20 New Mexico.

21 D. The legislature further declares that it would
22 have enacted the Consumer Information and Data Protection Act,
23 and each provision, section, subsection, sentence, clause,
24 phrase or word, and all constitutional applications of that
25 act, regardless of the fact that any provision, section,

.230941.5ms

1 subsection, sentence, clause, phrase or word, or applications
2 of that act, were to be declared unconstitutional or to
3 represent an undue burden.

4 E. If any provision of the Consumer Information and
5 Data Protection Act is found by any court to be
6 unconstitutionally vague, then the applications of that
7 provision that do not present constitutional vagueness problems
8 shall be severed and remain in force.

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
underscored material = new
[~~bracketed material~~] = delete