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:

underscored material = new
[~~bracketed material~~] = delete

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

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

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

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

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

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

(1) a digital or physical photograph;

(2) an audio or video recording; or

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

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

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

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

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

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

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

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

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

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

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

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

M. "covered platform" means any legal entity that:

(1) conducts business in New Mexico or produces or provides products or services that are targeted to residents of New Mexico;

(2) offers artificial intelligence or cloud computing services; and

(3) satisfies the following two thresholds:

(a) has gross annual revenues in excess of ten billion dollars ($10,000,000,000); and

(b) has at least fifty million United States-based monthly active users at any point during the twelve months preceding the filing of a complaint for an alleged violation of this act;

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

O. "dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making or choice and includes any practice the federal trade commission refers to as a "dark pattern";

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

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

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

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

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

R. "geofence" means any technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wireless fidelity technology data or any other form of location detection, or any combination of such coordinates, connectivity, data, identification or other form of location detection, to establish a virtual boundary;

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

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

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

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

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

U. "identified or identifiable individual" means an individual who can be readily identified, directly or indirectly;

V. "institution of higher education" means any individual who, or school, board, association, limited liability company or corporation that, is licensed or accredited to offer one or more programs of higher learning leading to one or more degrees;

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

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

Y. "online service, product or feature" means any service, product or feature that is provided online. "Online service, product or feature" does not include any:

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

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

(3) delivery or use of a physical product;

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

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

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

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

DD. "processor" means a person who processes personal data on behalf of a controller;

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

FF. "protected health information" has the same meaning as provided in HIPAA;

GG. "pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information; provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual;

HH. "publicly available information" means information that:

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

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

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

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

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

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

(4) a use or purchase of a medication, including, but not limited to, a medication used or purchased for the purposes of an abortion;

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

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

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

JJ. "reproductive or sexual health facility" means any health care facility in which at least seventy percent of the health care-related services or products rendered or provided in such facility are reproductive or sexual health care;

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

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

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

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

(4) the disclosure of personal data where the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a third party;

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

(6) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the third party assumes control of all or part of the

controller's assets;

LL. "sensitive data" means personal data that includes:

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

(2) consumer health data;

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

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

(5) an individual's account log-in, financial account, debit card or credit card number in combination with any required security or access code, password or credentials allowing access to an account;

(6) personal data collected from a known child;

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

(8) precise geolocation data;

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

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

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

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

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

NN. "third party" means a person, such as a public authority, agency or body, other than the consumer, controller or processor or an affiliate of the processor or the controller; and

OO. "verifiable covered resident request" means a request that is made by a covered resident, by a covered resident on behalf of the covered resident's minor child, by a natural person or a person registered with the secretary of state authorized by the covered resident to act on the covered resident's behalf or by a person who has power of attorney or is acting as a conservator for the covered resident and that the covered platform can verify, using commercially reasonable methods, to have the power of attorney or to be acting as a conservator for the covered resident about whom the covered platform has sensitive data. A covered platform is not obligated to provide information to a covered resident or to delete personal information if the covered platform cannot verify that the covered resident making the request is the covered resident about whom the covered platform has collected sensitive data or is a person authorized by the covered platform to act on the covered resident's behalf.

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

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

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

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

B. No person shall:

(1) provide any employee or contractor with access to consumer health data unless the employee or

contractor is subject to a contractual or statutory duty of confidentiality;

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

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

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

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

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

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

(3) covered entity or business associate governed by the privacy, security and breach notification rules issued by the federal department of health and human services,

45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the Health Information Technology for Economic and Clinical Health Act (P.L. 111-5);

(4) nonprofit organization; or

(5) institution of higher education.

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

(1) protected health information under HIPAA;

(2) patient identifying information for purposes of 42 U.S.C. Section 290dd-2;

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

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

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

(6) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to HIPAA;

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

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

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

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

(11) personal data regulated by the federal Family Educational Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g et seq.);

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

(13) data processed or maintained:

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

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

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

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

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

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

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

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

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

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

consumer.

B. A consumer may exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

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

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

(2) if a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but in all cases and at the latest within forty-five days of receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision pursuant to Subsection D of this section;

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

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

(5) a controller that has obtained personal data about a consumer from a source other than the consumer

shall be deemed in compliance with a consumer's request to delete such data pursuant to Paragraph (2) of Subsection A of this section by either:

(a) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business's records and not using such retained data for any other purpose pursuant to the provisions of the Consumer Information and Data Protection Act; or

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

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

D. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision pursuant to Paragraph (2) of Subsection C of this section. The appeal process shall be conspicuously available and similar to the process for submitting requests to initiate action pursuant to Subsection A of this section. Within sixty days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

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

SECTION 6. [NEW MATERIAL] DATA CONTROLLER

underscored material = new
[~~bracketed material~~] = delete

RESPONSIBILITIES--TRANSPARENCY.--

A. A controller shall:

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

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

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

(4) not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any of the consumer rights contained in the Consumer Information and Data Protection Act, including denying goods or services, charging different prices or rates for goods or services or providing a different level of quality

of goods and services to the consumer. However, nothing in this subsection shall be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out pursuant to Section 4 of the Consumer Information and Data Protection Act or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program; and

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

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

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

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

(2) the purpose for processing personal data;

(3) how consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

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

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

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

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

E. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under the Consumer Information and Data Protection Act. Such means shall take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of such requests and the ability of the controller to authenticate the identity of the consumer making the request. Controllers shall not require a consumer to create a new account in order to exercise consumer rights pursuant to Section 4 of the Consumer Information and Data Protection Act but may require a consumer to use an existing account.

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

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

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

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

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

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

(1) such precise geolocation data is reasonably necessary for the controller to provide an online service, product or feature and, if such data is necessary to provide such online service, product or feature, such controller shall only collect such data for the time necessary to provide such online service, product or feature; and

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

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

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

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

B. Subject to the consent requirement established in Subsection D of this section, no controller that offers any online service, product or feature to consumers whom the controller has actual knowledge or willfully disregards are minors younger than the age of eighteen shall:

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

(a) targeted advertising;

(b) any sale of personal data; or

(c) profiling in furtherance of any fully automated decision made by such controller that produces any legal or similarly significant effect concerning the provision or denial by such controller of any financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunity, health care services or access to essential goods or services, unless such processing is reasonably necessary to provide the online service, product or feature, or for any processing purpose other than the processing purpose that the controller disclosed at the time the controller collected the personal data, or that is reasonably necessary for, and compatible with, the processing purpose described in this subsection, or for longer than is reasonably necessary to provide the online service, product or feature; or

(2) use any system design feature to significantly increase, sustain or extend any minor younger than the age of eighteen's use of such online service, product or feature. The provisions of this subsection shall not apply to any service or application that is used by and under the direction of an educational entity, including a learning management system or a student engagement program.

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

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

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

D. No controller that offers any online service, product or feature to consumers whom the controller has actual knowledge or willfully disregards are minors younger than the age of eighteen shall engage in the activities described in Subsections B and C of this section unless the controller obtains the consent of the minor younger than the age of eighteen, or, if the minor is younger than thirteen years of age, the consent of the minor's parent or legal guardian. A controller that complies with the verifiable parental consent requirements established in the federal Children's Online Privacy Protection Act of 1998, 1S USC 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that act, as that act and the regulations, rules, guidance and exemptions may be amended from time to time, shall be deemed to have satisfied any requirement to obtain parental consent under this subsection.

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

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

(2) except as provided in Subsection F of this

section, offer any direct messaging apparatus for use by minors without providing readily accessible and easy-to-use safeguards to limit the ability of adults to send unsolicited communications to minors with whom they are not connected.

F. The provisions of Paragraph (2) of Subsection B of this section shall not apply to services when the predominant or exclusive function is:

(1) electronic mail; or

(2) direct messaging consisting of text, photos or videos that are sent between devices by electronic means, if messages are:

(a) shared between the sender and the recipient;

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

(c) not posted publicly.

SECTION 8. [NEW MATERIAL] DATA CONTROLLER RESPONSIBILITIES--ONLINE SERVICE, PRODUCT OR FEATURE--DATA PROTECTION ASSESSMENTS, REVIEW AND RECORD KEEPING.--

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

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

(2) that addresses:

(a) the purpose of the online service, product or feature;

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

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

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

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

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

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

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

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

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

D. If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment shall be deemed to satisfy the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

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

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

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

A. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting its obligations under the Consumer Information and Data Protection Act. Such assistance shall include:

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

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

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

B. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also include requirements that the processor shall:

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

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

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

(4) allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; alternatively, the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational

measures in support of the obligations under the Consumer Information and Data Protection Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request; and

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

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

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

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

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

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

(2) the sale of personal data;

(3) the processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of:

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

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

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

(d) other substantial injury to consumers;

(4) the processing of sensitive data; and

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

B. Data protection assessments conducted pursuant to Subsection A of this section shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks. The use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed, shall be factored into this assessment by the controller.

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

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

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

F. Data protection assessment requirements shall apply to processing activities created or generated after the effective date of the Consumer Information and Data Protection Act and are not retroactive.

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

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

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

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

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

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

C. Nothing in the Consumer Information and Data Protection Act shall be construed to require a controller or processor to comply with an authenticated consumer rights request, pursuant to Section 4 of the Consumer Information and Data Protection Act, if all of the following are true:

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

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

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

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

E. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments.

SECTION 12. [NEW MATERIAL] LIMITATIONS.--

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

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

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

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

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

(5) provide a product or service specifically requested by a consumer, perform a contract to which the consumer is a party, including fulfilling the terms of a

written warranty, or take steps at the request of the consumer prior to entering into a contract;

(6) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another natural person and where the processing cannot be manifestly based on another legal basis;

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

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

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

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

(c) if the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or

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

B. The obligations imposed on controllers or processors under the Consumer Information and Data Protection Act shall not restrict a controller's or processor's ability to collect, use or retain data to:

(1) conduct internal research to develop, improve or repair products, services or technology;

(2) effectuate a product recall;

(3) identify and repair technical errors that impair existing or intended functionality; or

(4) perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

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

D. A controller or processor that discloses personal data to a third-party controller or processor, in compliance with the requirements of the Consumer Information and Data Protection Act, is not in violation of that act if the third-party controller or processor that receives and processes such personal data is in violation of that act; provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of that act is likewise not in violation of that act for the transgressions of the controller or processor from which it receives such personal data.

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

F. Personal data processed by a controller pursuant to this section shall not be processed for any purpose other than those expressly listed in this section unless otherwise allowed by the Consumer Information and Data Protection Act. Personal data processed by a controller pursuant to this section may be processed to the extent that such processing is:

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

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

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

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

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

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

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

(1) delete the information in its possession; and

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

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

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

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

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

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

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

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

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

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

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

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

C. If a controller or processor continues to violate the Consumer Information and Data Protection Act following the cure period in Subsection B of this section or breaches an express written statement provided to the attorney general under that subsection, the attorney general may initiate an action and may seek an injunction to restrain any violations of that act and civil penalties of up to ten thousand dollars ($10,000) for each violation under that act.

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

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

SECTION 16. [<u>NEW MATERIAL</u>] SEVERABILITY.--

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

B. If any application of any provision in the Consumer Information and Data Protection Act to any person, group of persons or circumstances is found by a court to be invalid or unconstitutional, the remaining applications of that provision to all other persons and circumstances shall be severed and shall not be affected. All constitutionally valid applications of the Consumer Information and Data Protection Act shall be severed from any applications that a court finds to be invalid, leaving the valid applications in force, because it is the legislature's intent and priority that the valid applications be allowed to stand alone. Even if a reviewing court finds a provision of the Consumer Information and Data Protection Act to impose an undue burden in a large or substantial fraction of relevant cases, the applications that do not present an undue burden shall be severed from the remaining applications, shall remain in force and shall be treated as if the legislature had enacted a statute limited to the persons, group of persons or circumstances for which the statute's application does not present an undue burden.

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

D. The legislature further declares that it would have enacted the Consumer Information and Data Protection Act, and each provision, section, subsection, sentence, clause, phrase or word, and all constitutional applications of that act, regardless of the fact that any provision, section, subsection, sentence, clause, phrase or word, or applications of that act, were to be declared unconstitutional or to represent an undue burden.

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

F. No court may decline to enforce the severability requirements of Subsections A through E of this section on the ground that severance would rewrite the statute or involve the court in legislative or lawmaking activity. A court that declines to enforce or enjoins a state official from enforcing a statutory provision does not rewrite a statute, as the statute continues to contain the same words as before the court's decision. A judicial injunction or declaration of unconstitutionality:

(1) is nothing more than an edict prohibiting enforcement that may subsequently be vacated by a later court if that court has a different understanding of the requirements

of the constitution of New Mexico or the United States constitution;

(2) is not a formal amendment of the language in a statute; and

(3) no more rewrites a statute than a decision by the executive not to enforce a duly enacted statute in a limited and defined set of circumstances.