

1 HOUSE BILL 307

2 **57TH LEGISLATURE - STATE OF NEW MEXICO - FIRST SESSION, 2025**

3 INTRODUCED BY

4 Pamelya Herndon and Angelica Rubio and Andrea Romero
5 and Elizabeth "Liz" Stefanics
6
7
8
9

10 AN ACT

11 RELATING TO INTERNET SERVICES; ENACTING THE INTERNET PRIVACY
12 AND SAFETY ACT; ESTABLISHING REQUIREMENTS FOR SERVICE
13 PROVIDERS; PROHIBITING CERTAIN USES OF CONSUMER DATA; PROVIDING
14 RIGHTS TO CONSUMERS; ESTABLISHING LIMITATIONS ON PROCESSING OF
15 CONSUMER DATA; PROHIBITING WAIVERS OF RIGHTS AND RETALIATORY
16 DENIALS OF SERVICE; PROVIDING FOR INJUNCTIVE RELIEF AND CIVIL
17 PENALTIES; PROVIDING FOR RULEMAKING.

18
19 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

20 SECTION 1. [NEW MATERIAL] SHORT TITLE.--This act may be
21 cited as the "Internet Privacy and Safety Act".

22 SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the
23 Internet Privacy and Safety Act:

24 A. "actual knowledge" means a covered entity knows
25 that a consumer is a minor based upon:

.228900.4

underscored material = new
[bracketed material] = delete

1 (1) the self-identified age provided by the
2 minor, an age provided by a third party or an age or closely
3 related proxy that the covered entity knows or has associated
4 with, attributed to or derived or inferred for the consumer,
5 including for the purposes of advertising, marketing or product
6 development; or

7 (2) the consumer's use of an online feature,
8 product or service or a portion of such an online feature,
9 product or service that is directed to children;

10 B. "affiliate" means a legal entity that controls,
11 is controlled by or is under common control with another legal
12 entity;

13 C. "biometric data" means the data about a consumer
14 generated by measurements of the consumer's unique biological
15 characteristics, such as a faceprint, a fingerprint, a
16 voiceprint, a retina or an iris image or other biological
17 characteristic, that can be used to uniquely identify the
18 consumer. "Biometric data" does not include:

19 (1) demographic data;

20 (2) a donated portion of a human body stored
21 on behalf of a potential recipient of a living cadaveric
22 transplant and obtained or stored by a federally designated
23 organ procurement agency, including an artery, a bone, an eye,
24 an organ or tissue or blood or other fluid or serum;

25 (3) a human biological sample used for valid

1 scientific testing or screening;

2 (4) an image or film of the human anatomy used
3 to diagnose, provide a prognosis for or treat an illness or
4 other medical condition or to further validate scientific
5 testing or screening, including an x-ray, a roentgen process,
6 computed tomography, a magnetic resonance imaging image, a
7 positron emission tomography scan or mammography;

8 (5) information collected, used or stored for
9 health care treatment, payment or operations pursuant to
10 federal law governing health insurance;

11 (6) information collected, used or disclosed
12 for human subject research that is conducted in accordance with
13 the federal policy for the protection of human research ethics
14 laws or with internationally accepted clinical practice
15 guidelines as determined by the state department of justice by
16 rule;

17 (7) a photograph or video, except "biometric
18 data" includes data generated, captured or collected from the
19 biological characteristics of a consumer;

20 (8) a physical description, including height,
21 weight, hair color, eye color or a tattoo description; or

22 (9) a writing sample or written signature;

23 D. "brokerage of personal data" means the exchange
24 of personal data for monetary or other valuable consideration
25 by a covered entity to a third party, but does not include:

.228900.4

1 (1) the disclosure of personal data to a
2 service provider that processes the personal data on behalf of
3 the covered entity;

4 (2) the disclosure of personal data to a third
5 party for purposes of providing an online feature, product or
6 service requested by a consumer;

7 (3) the disclosure or transfer of personal
8 data to an affiliate of the covered entity;

9 (4) with the consumer's affirmative consent,
10 the disclosure of personal data where the consumer directs the
11 covered entity to disclose the personal data or intentionally
12 uses the covered entity to interact with a third party; or

13 (5) the disclosure of publicly available
14 information;

15 E. "collect" means accessing, acquiring or
16 gathering personal data;

17 F. "consumer" means a natural person who resides or
18 is present in New Mexico, including those identified by a
19 unique identifier;

20 G. "contextual advertising" means displaying or
21 presenting an advertisement that does not vary based on the
22 identity of the recipient and is based solely on:

23 (1) the immediate content of a web page or an
24 online feature, product or service within which the
25 advertisement appears;

.228900.4

1 (2) a specific request of a consumer for
2 information or feedback if displayed in proximity to the
3 results of such request for information; or

4 (3) a consumer's association with a geographic
5 area that is equal to or greater than the area of a circle with
6 a radius of ten miles;

7 H. "control" or "controlled" means:

8 (1) ownership of or the power to vote more
9 than fifty percent of the outstanding shares of a class of
10 voting security of a covered entity;

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

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

16 I. "covered entity" means a sole proprietorship,
17 partnership, limited liability company, corporation,
18 association, affiliate or other legal entity that:

19 (1) is organized or operated for the profit or
20 financial benefit of the entity's shareholders or other owners;

21 (2) offers online features, products or
22 services to consumers in New Mexico; and

23 (3) alone or jointly with others, determines
24 the purposes and means of:

25 (a) collecting personal data directly

1 from consumers;

2 (b) using personal data for targeted
3 advertising; or

4 (c) engaging in the brokerage of
5 personal data;

6 J. "dark pattern" means a user interface designed
7 or manipulated with the purpose of subverting or impairing user
8 autonomy, decision making or choice;

9 K. "default" means a preselected option adopted by
10 a covered entity for an online feature, product or service;

11 L. "de-identified data" means data that does not
12 identify and cannot be used to infer information about, or
13 otherwise be linked to, an identified or identifiable consumer
14 or a device linked to the consumer or that:

15 (1) takes reasonable physical, administrative
16 and technical measures to ensure that the data cannot be
17 associated with a consumer or be used to identify a consumer or
18 a device that identifies or is linked or reasonably linkable to
19 a consumer;

20 (2) publicly commits to process the data only
21 in a de-identified fashion; and

22 (3) contractually obligates a recipient of the
23 data to satisfy the requirements established pursuant to this
24 subsection;

25 M. "derived data" means data that is created by the

1 derivation of assumptions, conclusions, correlations, evidence,
2 data, inferences or predictions about a consumer or a
3 consumer's device from facts, evidence or other sources of
4 information;

5 N. "expressly provided personal data":

6 (1) means personal data provided by a consumer
7 to a covered entity expressly for purposes of a profile-based
8 feed to determine the order, relative prioritization, relative
9 prominence or selection of information that is furnished to the
10 consumer by the covered entity through an online product,
11 service or feature and includes:

12 (a) consumer-supplied filters, current
13 precise geolocation information supplied by the consumer,
14 resumption of a previous search, saved preferences and speech
15 patterns provided by the consumer for the purpose of enabling
16 the online product, service or feature to accept spoken input
17 or selecting the language in which the consumer interacts with
18 the online product, service or feature; and

19 (b) data submitted to a covered entity
20 by the consumer in order to receive particular information,
21 such as the social media profiles followed by the consumer,
22 video channels subscribed to by the consumer or other content
23 or sources of content on the online feature, product or service
24 the consumer has selected; and

25 (2) does not include:

1 (a) the history of a consumer's
2 connected device of browsing, device inactions, financial
3 transactions, geographical locations, physical activity or web
4 searches; or

5 (b) inferences about the consumer or the
6 consumer's connected device, including inferences based on data
7 described in Paragraph (1) of this subsection;

8 O. "first party" means a consumer-facing covered
9 entity with which the consumer intends or expects to interact;

10 P. "first-party advertising" means advertising or
11 marketing by a first party using first-party data and not other
12 forms of personal data and carried out:

13 (1) through direct communications with the
14 consumer, such as direct mail, email or text message
15 communications;

16 (2) in a physical location operated by the
17 first party; or

18 (3) through display or presentation of an
19 advertisement on the first party's own website, application or
20 other online content that promotes that first party's product
21 or service;

22 Q. "first-party data" means personal data collected
23 directly about a consumer by a first party, including data
24 collected during a consumer visit or use of a website, a
25 physical location or an online feature, product or service

1 operated by the first party;

2 R. "minor" means a consumer who is under eighteen
3 years of age;

4 S. "personal data" means information, including
5 derived data, that is linked or reasonably linkable, alone or
6 in combination with other information, to an identified or
7 identifiable consumer. "Personal data" does not include de-
8 identified information or publicly available information;

9 T. "precise geolocation" means data that is derived
10 from a device and that is used or intended to be used to reveal
11 the present or past geographical location of a consumer or a
12 consumer's device within a geographic area that is equal to or
13 smaller than the area of a circle with a radius of two thousand
14 feet;

15 U. "privacy-protective feed" means an algorithmic
16 ranking system that does not use the personal data of a
17 consumer to determine the order, relative prominence, relative
18 prioritization or selection of information that is furnished to
19 the consumer on an online feature, product or service except
20 for expressly provided personal data;

21 V. "profile-based feed" means an algorithmic
22 ranking system that determines the order, relative prominence,
23 relative prioritization, relative prominence or selection of
24 information that is furnished to a consumer on an online
25 feature, product or service based, in whole or part, on

.228900.4

1 personal data that is not expressly provided personal data;

2 W. "process" or "processing" means automated or
3 manual analysis, brokerage, collection, deletion, disclosure,
4 modification, storage, use, transfer or other handling of
5 personal data or sets of data;

6 X. "profiling" means automated processing of
7 personal data that uses personal data to evaluate certain
8 aspects relating to a consumer, including analyzing or
9 predicting aspects concerning the consumer's behavior, economic
10 situation, health, interests, location, movement, performance
11 at work, personal preferences or reliability. "Profiling" does
12 not include the processing of data that does not result in an
13 assessment or judgment about a consumer;

14 Y. "publicly available information", except the
15 information listed in Subsection Z of this section, means
16 information that has been lawfully made available to the
17 general public from:

18 (1) federal, state or municipal government
19 records;

20 (2) widely distributed media, including
21 personal data intentionally made available by a consumer to the
22 general public such that the consumer does not retain a
23 reasonable expectation of privacy in the personal data; or

24 (3) a disclosure that has been made to the
25 general public as required by federal, state or local law;

.228900.4

1 Z. "publicly available information" does not
2 include:

3 (1) an obscene visual depiction, as defined by
4 state law;

5 (2) personal data that is derived data from
6 multiple independent sources of publicly available information
7 that reveals sensitive personal data with respect to a
8 consumer;

9 (3) biometric data such that the consumer
10 retained a reasonable expectation of privacy in the
11 information;

12 (4) personal data that is created through the
13 combination of personal data with publicly available
14 information;

15 (5) genetic data, unless otherwise made
16 publicly available by the consumer to whom the information
17 pertains; or

18 (6) information made available by a consumer
19 on an online feature, product or service open to all members of
20 the public, whether for a fee or for free, where the consumer
21 has restricted the information to a specific audience in a
22 manner that the consumer would retain a reasonable expectation
23 of privacy for the information;

24 AA. "sensitive personal data" means personal data
25 that includes:

.228900.4

- 1 (1) biometric or genetic data;
- 2 (2) data revealing citizenship, ethnic origin,
3 immigration status or racial origin;
- 4 (3) financial data, including a credit card
5 number, a debit card number, a financial account number or
6 information that describes or reveals the bank account balances
7 or income level of a consumer, except that the last four digits
8 of a debit or credit card number are not sensitive personal
9 data;
- 10 (4) genetic or biometric data;
- 11 (5) a government-issued identifier, such as a
12 social security number, passport number or driver's license
13 number, that is not required by law to be displayed in public;
- 14 (6) data describing or revealing the past,
15 present or future mental or physical health of a consumer,
16 including:
- 17 (a) diagnosis;
- 18 (b) disability;
- 19 (c) health care condition; or
- 20 (d) treatment;
- 21 (7) data concerning the physical condition of
22 a consumer, including childbirth, pregnancy or a condition
23 related to childbirth or pregnancy;
- 24 (8) information about a consumer's personal
25 identity, including:

.228900.4

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

- 1 (a) ethnic or racial identity;
- 2 (b) gender and gender identity;
- 3 (c) sex;
- 4 (d) sex life; or
- 5 (e) sexual orientation;
- 6 (9) precise geolocation;
- 7 (10) religious affiliation; or
- 8 (11) union membership;

9 BB. "service provider" means a person who collects,
10 processes, retains or transfers personal data on behalf of, and
11 at the direction of, a covered entity or a service provider;

12 CC. "targeted advertising" means displaying or
13 presenting an online advertisement to a consumer or to a device
14 identified by a unique persistent identifier or to a group of
15 consumers or devices identified by unique persistent
16 identifiers when the advertisement is selected based, in whole
17 or in part, on known or predicted preferences, characteristics,
18 behavior or interests associated with the consumer or a device
19 identified by a unique persistent identifier. "Targeted
20 advertising" does not include first-party advertising or
21 contextual advertising; and

22 DD. "third party" means a person or entity other
23 than the consumer of the covered entity, the covered entity or
24 a service provider for the covered entity.

25 SECTION 3. [NEW MATERIAL] REQUIREMENTS FOR COVERED

.228900.4

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

1 ENTITIES--ONLINE PLATFORMS--CONSUMER OPTIONS--MINORS.--

2 A. Except as provided in Subsection B of this
3 section, a covered entity shall:

4 (1) configure all default privacy settings on
5 the covered entity's online platforms offering features,
6 products or services to settings that offer the highest level
7 of privacy;

8 (2) publicly provide privacy information,
9 terms of service, policies and community standards in a
10 prominent, precise manner and use clear, easily understood
11 language;

12 (3) publicly provide prominent, accessible and
13 responsive tools to help a consumer exercise the consumer's
14 privacy rights and report concerns; and

15 (4) establish, implement and maintain
16 reasonable administrative, technical and physical data security
17 practices to protect the confidentiality, integrity and
18 accessibility of personal data appropriate to the volume and
19 nature of the personal data at issue pursuant to guidelines
20 established by the state department of justice by rule.

21 B. When a covered entity does not have actual
22 knowledge that a consumer using the covered entity's online
23 platform to access a feature, product or service is a minor,
24 the covered entity shall establish settings on that online
25 platform that:

.228900.4

1 (1) permit a consumer to disable notifications
2 or disable notifications during specific periods of time;

3 (2) permit a consumer to choose between a
4 privacy-protective feed and a profile-based feed; and

5 (3) permit a consumer to disable contact by
6 unknown individuals unless the consumer first initiates the
7 contact or provide a mechanism to screen contact by individuals
8 with whom the consumer does not have a relationship.

9 C. When a covered entity has actual knowledge that
10 a consumer using the covered entity's online platform is a
11 minor, the covered entity shall establish default settings on
12 the platform:

13 (1) that disable contact by unknown users
14 unless the consumer first initiates the contact;

15 (2) that disable notifications between the
16 hours of 10:00 p.m. and 6:00 a.m. mountain time pursuant to
17 federal law; and

18 (3) that use a privacy-protective feed.

19 SECTION 4. [NEW MATERIAL] PROHIBITED PRACTICES--CONSUMER
20 OPT-IN OPTION.--A covered entity that provides an online
21 feature, product or service that involves the processing of
22 personal data shall not, and shall not instruct a service
23 provider or third party, to:

24 A. profile a consumer by default, unless profiling
25 is necessary to provide the online feature, product or service

1 requested, and only with respect to the aspects of the online
2 feature, product or service with which the consumer is actively
3 and knowingly engaged;

4 B. process the personal data of a consumer except
5 as necessary to provide:

6 (1) the specific online feature, product or
7 service with which the consumer is actively and knowingly
8 engaged, including any routine administrative, operational or
9 account-servicing activity, such as billing, shipping,
10 delivery, storage, accounting, security or fraud detection; or

11 (2) a communication, that is not an
12 advertisement, by the covered entity to the consumer that is
13 reasonably anticipated within the context of the relationship
14 between the covered entity and the consumer;

15 C. process personal data for any reason other than
16 a reason for which the personal data is collected;

17 D. process a consumer's sensitive personal data
18 unless the collection of that data is strictly necessary for
19 the covered entity to provide the online feature, product or
20 service requested and then only for the limited time that the
21 collection of data is necessary to provide the online feature,
22 product or service;

23 E. process a consumer's precise geolocation
24 information without providing an obvious signal to the consumer
25 for the duration of that collection that precise geolocation

.228900.4

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

1 information is being collected;

2 F. use dark patterns to cause a consumer to provide
3 personal data beyond what is reasonably expected to provide the
4 online feature, product or service, to forego privacy
5 protections;

6 G. allow a person to monitor a consumer's online
7 activity or precise geolocation without providing an obvious
8 signal to the consumer that the consumer is being monitored or
9 tracked;

10 H. process or transfer personal data in a manner
11 that discriminates in or otherwise makes unavailable the equal
12 enjoyment of goods or services on the basis of childbirth or
13 condition related to pregnancy or childbirth, color,
14 disability, gender, gender identity, mental health, national
15 origin, physical health condition or diagnosis, race,
16 religion, sex life or sexual orientation;

17 I. process personal data for purposes of targeted
18 advertising, first-party advertising or the brokerage of
19 personal data without the consumer first opting in to those
20 purposes by clear and conspicuous means and not through the use
21 of dark patterns; or

22 J. process sensitive personal data for purposes of
23 targeted advertising, first-party advertising or the brokerage
24 of personal data.

25 SECTION 5. [NEW MATERIAL] RIGHTS OF ACCESS--CORRECTION--

.228900.4

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

1 DELETION.--

2 A. Covered entities shall provide a consumer the
3 right to:

4 (1) access all the consumer's personal data
5 that was processed by the covered entity or a service provider;

6 (2) access all the information pertaining to
7 the collection and processing of the consumer's personal
8 information, including:

9 (a) where or from whom the covered
10 entity obtained personal data, such as whether the information
11 was obtained from the consumer or a third party or from an
12 online or offline source;

13 (b) the types of third parties to which
14 the covered entity has disclosed or will disclose personal
15 data;

16 (c) the purposes of the processing;

17 (d) the categories of personal data
18 concerned;

19 (e) the names of third parties to which
20 the covered entity had disclosed the personal data and a log
21 showing when such disclosure happened; and

22 (f) the period of retention of the
23 personal data;

24 (3) obtain the consumer's personal data
25 processed by a covered entity in a structured, readily usable,

.228900.4

1 portable and machine-readable format;

2 (4) transmit or cause the covered entity to
3 transmit the consumer's personal data to another covered
4 entity, where technically feasible;

5 (5) request a covered entity to stop
6 collecting and processing the consumer's personal data;

7 (6) correct inaccurate personal data stored by
8 covered entities; and

9 (7) delete the consumer's personal data that
10 is stored by covered entities, including from nonpublic
11 profiles; provided that a covered entity that has collected
12 personal data from a consumer is not required to delete
13 information to the extent that the covered entity is exempt
14 under Section 9 of the Internet Privacy and Safety Act.

15 B. A covered entity shall provide a consumer with a
16 reasonable means to exercise the consumer's rights pursuant to
17 Subsection A of this section in a request form that is:

18 (1) clear and conspicuous;

19 (2) made available at no additional cost and
20 with no transactional penalty to the consumer to whom the
21 information pertains; and

22 (3) in English or another language in which
23 the covered entity communicates with the consumer to whom the
24 information pertains.

25 C. A covered entity shall comply with a consumer's

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

1 request to exercise the consumer's rights pursuant to
2 Subsection A or B of this section within thirty days after
3 receiving a verifiable request; provided that:

4 (1) when the covered entity has a reasonable
5 doubt or cannot verify the identity of the consumer making a
6 request, the covered entity may request additional personal
7 information necessary for the specific purpose of confirming
8 the consumer's identity; and

9 (2) the covered entity shall not de-identify
10 the consumer's personal data for sixty days from the date on
11 which the covered entity receives a request for correction or
12 deletion from the consumer pursuant to this section.

13 SECTION 6. [NEW MATERIAL] DATA PROCESSING AGREEMENTS.--

14 A. A service provider that processes personal data
15 on behalf of a covered entity or another service provider or a
16 third party that receives personal data from a covered entity
17 shall enter into a written data processing agreement with the
18 covered entity ensuring that the data will continue to be
19 processed consistent with the Internet Privacy and Safety Act.
20 The agreement shall specify that:

21 (1) personal data received by service
22 providers or third parties shall be processed only for purposes
23 specified by the covered entity in the data processing
24 agreement, subject to the limitations of the Internet Privacy
25 and Safety Act;

.228900.4

underscored material = new
[bracketed material] = delete

1 (2) service providers and third parties shall
2 only process personal data that is adequate, relevant and
3 necessary for the purposes for which the data was collected or
4 received;

5 (3) service providers and third parties shall
6 ensure that subcontractors comply with the same data protection
7 obligations as set forth in their data processing agreement
8 with the covered entity;

9 (4) service providers and third parties shall
10 establish, implement and maintain reasonable administrative,
11 technical and physical data security practices to protect the
12 confidentiality, integrity and accessibility of personal data
13 appropriate to the volume and nature of the personal data at
14 issue; and

15 (5) service providers shall adhere to the
16 instructions of a controller and shall assist the controller in
17 meeting the controller's obligations pursuant to the Internet
18 Privacy and Safety Act.

19 B. Prior to transferring personal data to a third
20 party located outside of New Mexico, covered entities shall
21 ensure that adequate data protection safeguards consistent with
22 the Internet Privacy and Safety Act are in place.

23 SECTION 7. [NEW MATERIAL] PROHIBITION ON WAIVING OF
24 RIGHTS AND RETALIATORY DENIAL OF SERVICE.--

25 A. A covered entity shall not retaliate against a

.228900.4

underscoring material = new
[bracketed material] = delete

1 consumer for exercising a right guaranteed by the Internet
2 Privacy and Safety Act, or a rule promulgated under that act,
3 including charging different prices or rates for goods and
4 services, denying goods or services or providing a different
5 level of quality of goods or services.

6 B. A provision of a contract, an agreement or terms
7 of service shall not waive, limit or otherwise undermine the
8 rights conferred under the Internet Privacy and Safety Act or
9 other applicable data protection laws.

10 C. A provision within a contract or an agreement
11 between a covered entity and a consumer that is invalid or
12 unenforceable pursuant to the Internet Privacy and Safety Act
13 shall not affect the validity or enforceability of the
14 remaining provisions of the contract or agreement.

15 SECTION 8. [NEW MATERIAL] VIOLATIONS--ENFORCEMENT--
16 PENALTIES--CLAIMS FOR VIOLATIONS.--Upon promulgation of rules
17 by the state department of justice to implement the Internet
18 Privacy and Safety Act:

19 A. a covered entity that violates the provisions of
20 that act shall be:

21 (1) subject to injunctive relief to cease or
22 correct the violation;

23 (2) liable for a civil penalty of not more
24 than two thousand five hundred dollars (\$2,500) per affected
25 consumer for each negligent violation; and

.228900.4

underscoring material = new
[bracketed material] = delete

1 (3) liable for a civil penalty of not more
2 than seven thousand five hundred dollars (\$7,500) per affected
3 consumer for each intentional violation; and

4 B. a consumer who claims to have suffered a
5 deprivation of the rights secured under that act may maintain
6 an action to establish liability and recover damages or
7 equitable or injunctive relief in district court.

8 SECTION 9. [NEW MATERIAL] EXCEPTIONS.--

9 A. A covered entity that is in compliance with
10 federal privacy laws shall be deemed to be in compliance with
11 the requirements of the Internet Privacy and Safety Act solely
12 and exclusively with respect to data subject to the
13 requirements of federal law.

14 B. An online feature, product or service that is
15 regulated pursuant to federal information security law shall be
16 deemed to be in compliance with the requirements of the
17 Internet Privacy and Safety Act solely and exclusively with
18 respect to data subject to the requirements of federal law.

19 C. The Internet Privacy and Safety Act does not
20 apply to the delivery or use of a physical product to the
21 extent the product is not an online feature, product or
22 service.

23 SECTION 10. [NEW MATERIAL] LIMITATIONS.--Nothing in the
24 Internet Privacy and Safety Act shall be interpreted or
25 construed to:

.228900.4

1 A. impose liability in a manner that is
2 inconsistent with federal law;

3 B. apply to information processed by local, state,
4 or federal government or municipal corporations; or

5 C. restrict a covered entity's or service
6 provider's ability to:

7 (1) comply with federal or New Mexico law;

8 (2) comply with a civil or criminal subpoena
9 or summons, except as prohibited by New Mexico law;

10 (3) cooperate with law enforcement agencies
11 concerning conduct or activity that the covered entity or
12 service provider reasonably and in good faith believes may
13 violate federal, state or municipal ordinances or regulations;

14 (4) investigate, establish, exercise, prepare
15 for or defend legal claims to the extent that the regulated
16 data is relevant to the parties' claims;

17 (5) take immediate steps to protect the life
18 or physical safety of a consumer or another individual in an
19 emergency, and where the processing cannot be manifestly based
20 on another legal basis; provided that a consumer's access to
21 health care services lawful in the state of New Mexico shall
22 not constitute an emergency;

23 (6) prevent, detect, protect against or
24 respond to security incidents relating to network security or
25 physical security, including an intrusion or trespass, medical

1 alert or request for a medical response, fire alarm or request
2 for a fire response, or access control;

3 (7) prevent, detect, protect against or
4 respond to identity theft, fraud, harassment, malicious or
5 deceptive activities or illegal activity targeted at or
6 involving the covered entity or service provider or its
7 services, preserve the integrity or security of systems or
8 investigate, report or prosecute those responsible for any such
9 action;

10 (8) assist another covered entity, service
11 provider or third party with any of the obligations in the
12 Internet Privacy and Safety Act;

13 (9) transfer assets to a third party in the
14 context of a merger, acquisition, bankruptcy or similar
15 transaction when the third party assumes control, in whole or
16 in part, of the covered entity's assets, only if the covered
17 entity, in a reasonable time prior to the transfer, provides an
18 affected consumer with a notice describing the transfer,
19 including the name of the entity receiving the consumer's
20 regulated health data and the applicable privacy policies of
21 such entity; or

22 (10) transfer assets to a third party in the
23 context of a merger, acquisition, bankruptcy or similar
24 transaction when the third party assumes control, in whole or
25 in part, of the covered entity's assets, only if the covered

.228900.4

underscored material = new
[bracketed material] = delete

1 entity, in a reasonable time prior to the transfer, provides an
2 affected consumer with a reasonable opportunity to:

3 (a) withdraw previously provided consent
4 or opt-ins related to the consumer's personal data;

5 (b) request the deletion of the
6 consumer's regulated health data;

7 (c) meet federal law requirements for
8 data used or collected for medical research; or

9 (d) with respect to personal data
10 previously collected in accordance with the Internet Privacy
11 and Safety Act, process that regulated health data solely for
12 the purpose that the regulated health data becomes
13 de-identified data.

14 SECTION 11. [NEW MATERIAL] STATE DEPARTMENT OF JUSTICE--
15 RULEMAKING--REPORTS.--

16 A. On or before April 1, 2026, the state department
17 of justice shall promulgate rules for the implementation of the
18 Internet Privacy and Safety Act.

19 B. On or before November 30, 2026 and on or before
20 November 30 in each subsequent year, the state department of
21 justice shall provide a report to the interim legislative
22 committee that is tasked with examining internet-related
23 issues. The report shall:

24 (1) compare the requirements of the then-
25 current federal laws and regulations with the requirements of

.228900.4

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

1 the Internet Privacy and Safety Act and the rules promulgated
2 pursuant to Subsection A of this section on entities offering
3 online features, products or services concerning data privacy
4 and the protection of minors; and

5 (2) provide recommendations for statutory
6 changes needed to conform state law with federal law.

7 - 27 -
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25