

1 SENATE BILL 420

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

3 INTRODUCED BY

4 Katy M. Duhigg and Angel M. Charley and Christine Chandler  
5 and Pamela Herndon  
6  
7  
8  
9

10 AN ACT

11 RELATING TO INTERNET SERVICES; ENACTING THE COMMUNITY 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 "Community Privacy and Safety Act".

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

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

.230898.1

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:

.230898.1

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;

.230898.1

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 of the covered entity that  
15 possesses the data that:

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

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

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

.230898.1

1 M. "derived data" means data that is created by the  
2 derivation of assumptions, conclusions, correlations, evidence,  
3 data, inferences or predictions about a consumer or a  
4 consumer's device from facts, evidence or other sources of  
5 information;

6 N. "expressly provided personal data":

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

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

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

.230898.1

1 (2) does not include:

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

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

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

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

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

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

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

23 Q. "first-party data" means personal data collected  
24 directly about a consumer by a first party, including data  
25 collected during a consumer visit or use of a website, a



1 physical location or an online feature, product or service  
2 operated by the first party;

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

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

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

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

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

1 service based, in whole or part, on personal data that is not  
2 expressly provided personal data;

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

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

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

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

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

25 (3) a disclosure that has been made to the

1 general public as required by federal, state or local law;

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

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

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

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

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

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

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

25 AA. "sensitive personal data" means personal data

1 that includes:

2 (1) biometric or genetic data;

3 (2) data revealing citizenship, ethnic origin,  
4 immigration status or racial origin;

5 (3) financial data, including a credit card  
6 number, a debit card number, a financial account number or  
7 information that describes or reveals the bank account balances  
8 or income level of a consumer, except that the last four digits  
9 of a debit or credit card number are not sensitive personal  
10 data;

11 (4) 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 (5) 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 (6) data concerning the physical condition of  
22 a consumer, including childbirth, pregnancy or a condition  
23 related to childbirth or pregnancy;

24 (7) information about a consumer's personal  
25 identity, including:

.230898.1

- 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 (8) precise geolocation;
- 7 (9) religious affiliation; or
- 8 (10) 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. "small business" means a covered entity or  
13 service provider that, for the period of the three preceding  
14 calendar years or for the period during which the covered  
15 entity or service provider has been in existence if that period  
16 is less than three years, meets the following criteria:

17 (1) the covered entity or service provider did  
18 not annually process the personal data of more than fifteen  
19 thousand consumers during the period for any purpose other than  
20 initiating, rendering, billing for, finalizing, completing or  
21 otherwise collecting payment for a requested service or  
22 product; and

23 (2) the covered entity or service provider did  
24 not engage in brokerage of personal data, except for purposes  
25 of initiating, rendering, billing for, finalizing, completing

underscoring material = new  
[bracketed material] = delete

1 or otherwise collecting payment for a requested service or  
2 product;

3 DD. "targeted advertising" means displaying or  
4 presenting an online advertisement to a consumer or to a device  
5 identified by a unique persistent identifier or to a group of  
6 consumers or devices identified by unique persistent  
7 identifiers when the advertisement is selected based, in whole  
8 or in part, on known or predicted preferences, characteristics,  
9 behavior or interests associated with the consumer or a device  
10 identified by a unique persistent identifier. "Targeted  
11 advertising" does not include first-party advertising or  
12 contextual advertising; and

13 EE. "third party" means a person or entity other  
14 than the consumer of the covered entity, the covered entity or  
15 a service provider for the covered entity.

16 SECTION 3. [NEW MATERIAL] REQUIREMENTS FOR COVERED  
17 ENTITIES--ONLINE PLATFORMS--CONSUMER OPTIONS--MINORS.--

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

20 (1) configure all default privacy settings on  
21 the covered entity's online platforms offering features,  
22 products or services to settings that offer the highest level  
23 of privacy;

24 (2) publicly provide privacy information,  
25 terms of service, policies and community standards in a

1 prominent, precise manner and use clear, easily understood  
2 language;

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

6 (4) establish, implement and maintain  
7 reasonable administrative, technical and physical data security  
8 practices to protect the confidentiality, integrity and  
9 accessibility of personal data appropriate to the volume and  
10 nature of the personal data at issue pursuant to guidelines  
11 established by the state department of justice by rule.

12 B. When a covered entity does not have actual  
13 knowledge that a consumer using the covered entity's online  
14 platform to access a feature, product or service is a minor,  
15 the covered entity shall establish settings on that online  
16 platform that:

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

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

21 (3) permit a consumer to disable contact by  
22 unknown individuals unless the consumer first initiates the  
23 contact or provide a mechanism to screen contact by individuals  
24 with whom the consumer does not have a relationship.

25 C. When a covered entity has actual knowledge that

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

1 a consumer using the covered entity's online platform is a  
2 minor, the covered entity shall establish default settings on  
3 the platform:

4 (1) that disable contact by unknown users  
5 unless the consumer first initiates the contact;

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

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

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

15 A. profile a consumer by default, unless profiling  
16 is necessary to provide the online feature, product or service  
17 requested, and only with respect to the aspects of the online  
18 feature, product or service with which the consumer is actively  
19 and knowingly engaged;

20 B. process the personal data of a consumer except  
21 as necessary to provide:

22 (1) the specific online feature, product or  
23 service with which the consumer is actively and knowingly  
24 engaged, including any routine administrative, operational or  
25 account-servicing activity, such as billing, shipping,

.230898.1



1 delivery, storage, accounting, security or fraud detection; or

2 (2) a communication, that is not an  
3 advertisement, by the covered entity to the consumer that is  
4 reasonably anticipated within the context of the relationship  
5 between the covered entity and the consumer;

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

8 D. process a consumer's sensitive personal data  
9 unless the collection of that data is strictly necessary for  
10 the covered entity to provide the online feature, product or  
11 service requested and then only for the limited time that the  
12 collection of data is necessary to provide the online feature,  
13 product or service;

14 E. process a consumer's precise geolocation  
15 information without providing an obvious signal to the consumer  
16 for the duration of that collection that precise geolocation  
17 information is being collected;

18 F. use dark patterns to cause a consumer to provide  
19 personal data beyond what is reasonably expected to provide the  
20 online feature, product or service, to forego privacy  
21 protections;

22 G. allow a person to monitor a consumer's online  
23 activity or precise geolocation without providing an obvious  
24 signal to the consumer that the consumer is being monitored or  
25 tracked;

.230898.1

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

1 H. process or transfer personal data in a manner  
2 that discriminates in or otherwise makes unavailable the equal  
3 enjoyment of goods or services on the basis of childbirth or  
4 condition related to pregnancy or childbirth, color,  
5 disability, gender, gender identity, mental health, national  
6 origin, physical health condition or diagnosis, race,  
7 religion, sex life or sexual orientation;

8 I. process personal data for purposes of targeted  
9 advertising, first-party advertising or the brokerage of  
10 personal data without the consumer first opting in to those  
11 purposes by clear and conspicuous means and not through the use  
12 of dark patterns; or

13 J. process sensitive personal data for purposes of  
14 targeted advertising, first-party advertising or the brokerage  
15 of personal data.

16 SECTION 5. [NEW MATERIAL] RIGHTS OF ACCESS--CORRECTION--  
17 DELETION.--

18 A. Covered entities shall provide a consumer the  
19 right to:

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

22 (2) access all the information pertaining to  
23 the collection and processing of the consumer's personal  
24 information, including:

25 (a) where or from whom the covered

1 entity obtained personal data, such as whether the information  
2 was obtained from the consumer or a third party or from an  
3 online or offline source;

4 (b) the types of third parties to which  
5 the covered entity has disclosed or will disclose personal  
6 data;

7 (c) the purposes of the processing;

8 (d) the categories of personal data  
9 concerned;

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

13 (f) the period of retention of the  
14 personal data;

15 (3) obtain the consumer's personal data  
16 processed by a covered entity in a structured, readily usable,  
17 portable and machine-readable format;

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

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

23 (6) correct inaccurate personal data stored by  
24 covered entities; and

25 (7) delete the consumer's personal data that

1 is stored by covered entities, including from nonpublic  
2 profiles; provided that a covered entity that has collected  
3 personal data from a consumer is not required to delete  
4 information to the extent that the covered entity is exempt  
5 under Section 9 of the Community Privacy and Safety Act.

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

9 (1) clear and conspicuous;

10 (2) made available at no additional cost and  
11 with no transactional penalty to the consumer to whom the  
12 information pertains; and

13 (3) in English or another language in which  
14 the covered entity communicates with the consumer to whom the  
15 information pertains.

16 C. A covered entity shall comply with a consumer's  
17 request to exercise the consumer's rights pursuant to  
18 Subsection A or B of this section within thirty days after  
19 receiving a verifiable request; provided that:

20 (1) when the covered entity has a reasonable  
21 doubt or cannot verify the identity of the consumer making a  
22 request, the covered entity may request additional personal  
23 information necessary for the specific purpose of confirming  
24 the consumer's identity; and

25 (2) the covered entity shall not de-identify

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

1 the consumer's personal data for sixty days from the date on  
2 which the covered entity receives a request for correction or  
3 deletion from the consumer pursuant to this section.

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

5 A. A service provider that processes personal data  
6 on behalf of a covered entity or another service provider or a  
7 third party that receives personal data from a covered entity  
8 shall enter into a written data processing agreement with the  
9 covered entity ensuring that the data will continue to be  
10 processed consistent with the Community Privacy and Safety Act.  
11 The agreement shall specify that:

12 (1) personal data received by service  
13 providers or third parties shall be processed only for purposes  
14 specified by the covered entity in the data processing  
15 agreement, subject to the limitations of the Community Privacy  
16 and Safety Act;

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

21 (3) service providers and third parties shall  
22 ensure that subcontractors comply with the same data protection  
23 obligations as set forth in their data processing agreement  
24 with the covered entity;

25 (4) service providers and third parties shall

.230898.1

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

1 establish, implement and maintain reasonable administrative,  
2 technical and physical data security practices to protect the  
3 confidentiality, integrity and accessibility of personal data  
4 appropriate to the volume and nature of the personal data at  
5 issue; and

6 (5) service providers shall adhere to the  
7 instructions of a covered entity and shall assist the covered  
8 entity in meeting the covered entity's obligations pursuant to  
9 the Community Privacy and Safety Act.

10 B. Prior to transferring personal data to a third  
11 party located outside of New Mexico, covered entities shall  
12 ensure that adequate data protection safeguards consistent with  
13 the Community Privacy and Safety Act are in place.

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

16 A. A covered entity shall not retaliate against a  
17 consumer for exercising a right guaranteed by the Community  
18 Privacy and Safety Act, or a rule promulgated under that act,  
19 including charging different prices or rates for goods and  
20 services, denying goods or services or providing a different  
21 level of quality of goods or services.

22 B. A provision of a contract, an agreement or terms  
23 of service shall not waive, limit or otherwise undermine the  
24 rights conferred under the Community Privacy and Safety Act or  
25 other applicable data protection laws.

.230898.1

underscoring material = new  
[bracketed material] = delete

1 C. A provision within a contract or an agreement  
2 between a covered entity and a consumer that is invalid or  
3 unenforceable pursuant to the Community Privacy and Safety Act  
4 shall not affect the validity or enforceability of the  
5 remaining provisions of the contract or agreement.

6 SECTION 8. [NEW MATERIAL] VIOLATIONS--ENFORCEMENT--  
7 PENALTIES--CLAIMS FOR VIOLATIONS.--Upon promulgation of rules  
8 by the state department of justice to implement the Community  
9 Privacy and Safety Act:

10 A. a covered entity that violates the provisions of  
11 that act shall be:

12 (1) subject to injunctive relief to cease or  
13 correct the violation;

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

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

20 B. a consumer who claims to have suffered a  
21 deprivation of the rights secured under the Community Privacy  
22 and Safety Act may maintain an action to establish liability  
23 and recover damages or equitable or injunctive relief in  
24 district court; and

25 C. for a period of three years immediately

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

1 following the date of enactment of the Community Privacy and  
2 Safety Act, an action under this section shall not be  
3 maintained against a small business unless the maintaining  
4 party first provides the small business with a notice  
5 reasonably describing the alleged violation or deprivation of  
6 rights under that act and providing a sixty-day opportunity to  
7 cure. If the small business fails to cure the violation within  
8 sixty days of receipt of the notice of violation, an action may  
9 be maintained pursuant to this section without further notice.

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

11 A. A covered entity that is in compliance with  
12 federal privacy laws shall be deemed to be in compliance with  
13 the requirements of the Community Privacy and Safety Act solely  
14 and exclusively with respect to data subject to the  
15 requirements of federal law; provided that a covered entity  
16 that is in compliance with the federal Children's Online  
17 Privacy Protection Act of 1998 shall be in compliance with the  
18 requirements of the Community Privacy and Safety Act only to  
19 the extent that compliance with that act is inconsistent with  
20 the federal Children's Online Privacy Protection Act of 1998.

21 B. An online feature, product or service that is  
22 regulated pursuant to federal information security law shall be  
23 deemed to be in compliance with the requirements of the  
24 Community Privacy and Safety Act solely and exclusively with  
25 respect to data subject to the requirements of federal law.

.230898.1



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

1           C. The Community Privacy and Safety Act does not  
2 apply to the delivery or use of a physical product to the  
3 extent the product is not an online feature, product or  
4 service.

5           **SECTION 10. [NEW MATERIAL] LIMITATIONS.**--Nothing in the  
6 Community Privacy and Safety Act shall be interpreted or  
7 construed to:

8           A. impose liability in a manner that is  
9 inconsistent with federal law;

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

12           C. restrict a covered entity's or service  
13 provider's ability to:

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

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

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

21                   (4) investigate, establish, exercise, prepare  
22 for or defend legal claims to the extent that the personal data  
23 is relevant to the parties' claims;

24                   (5) take immediate steps to protect the life  
25 or physical safety of a consumer or another individual in an

.230898.1

1 emergency, and where the processing cannot be manifestly based  
2 on another legal basis; provided that a consumer's access to  
3 health care services lawful in the state of New Mexico shall  
4 not constitute an emergency;

5 (6) prevent, detect, protect against or  
6 respond to security incidents relating to network security or  
7 physical security, including an intrusion or trespass, medical  
8 alert or request for a medical response, fire alarm or request  
9 for a fire response, or access control;

10 (7) prevent, detect, protect against or  
11 respond to identity theft, fraud, harassment, malicious or  
12 deceptive activities or illegal activity targeted at or  
13 involving the covered entity or service provider or its  
14 services, preserve the integrity or security of systems or  
15 investigate, report or prosecute those responsible for any such  
16 action;

17 (8) assist another covered entity, service  
18 provider or third party with any of the obligations in the  
19 Community Privacy and Safety Act;

20 (9) transfer assets to a third party in the  
21 context of a merger, acquisition, bankruptcy or similar  
22 transaction when the third party assumes control, in whole or  
23 in part, of the covered entity's assets, only if the covered  
24 entity, in a reasonable time prior to the transfer, provides an  
25 affected consumer with notice describing the transfer,

.230898.1

underscored material = new  
[bracketed material] = delete

1 including the name of the entity receiving the consumer's  
2 personal data and the applicable privacy policies of the  
3 entity, and a reasonable opportunity to:

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

6 (b) request the deletion of the  
7 consumer's personal data;

8 (10) meet federal law requirements for data  
9 used or collected for medical research; or

10 (11) process personal data previously  
11 collected in accordance with the Community Privacy and Safety  
12 Act, solely for the purpose of the personal data becoming  
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 Community 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

.230898.1

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

1 the Community 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 - 28 -  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25