HOUSE BILL 307

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

INTRODUCED BY

Pamelya Herndon and Angelica Rubio

AN ACT

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

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 "Internet Privacy and Safety Act".

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

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

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

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

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

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

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

(1) demographic data;

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

(3) a human biological sample used for valid

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

scientific testing or screening;

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

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

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

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

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

(9) a writing sample or written signature;

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

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

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

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

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

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

(5) the disclosure of publicly available information;

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

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

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

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

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

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

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

H. "control" or "controlled" means:

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

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

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

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

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

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

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

(a) collecting personal data directly

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

from consumers;

(b) using personal data for targeted advertising; or

(c) engaging in the brokerage of personal data;

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

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

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

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

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

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

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

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

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

N. "expressly provided personal data":

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

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

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

(2) does not include:

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

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

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

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

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

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

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

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

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

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

operated by the first party;

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

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

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

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

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

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

personal data that is not expressly provided personal data;

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

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

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

(1) federal, state or municipal government records;

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

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

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

Z. "publicly available information" does not include:

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

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

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

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

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

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

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

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

(1) biometric or genetic data;

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

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

(4) genetic or biometric data;

(5) a government-issued identifier, such as a social security number, passport number or driver's license number, that is not required by law to be displayed in public;

(6) data describing or revealing the past, present or future mental or physical health of a consumer, including:

(a) diagnosis;

(b) disability;

(c) health care condition; or

(d) treatment;

(7) data concerning the physical condition of a consumer, including childbirth, pregnancy or a condition related to childbirth or pregnancy;

(8) information about a consumer's personal identity, including:

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

(a) ethnic or racial identity;

(b) gender and gender identity;

(c) sex;

(d) sex life; or

(e) sexual orientation;

(9) precise geolocation;

(10) religious affiliation; or

(11) union membership;

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

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

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

SECTION 3. [NEW MATERIAL] REQUIREMENTS FOR COVERED

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) that use a privacy-protective feed.

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

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

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

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

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

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

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

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

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

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

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

information is being collected;

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

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

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

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

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

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

DELETION.--

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

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

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

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

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

(c) the purposes of the processing;

(d) the categories of personal data concerned;

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

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

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

portable and machine-readable format;

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

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

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

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

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

(1) clear and conspicuous;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. A covered entity shall not retaliate against a

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

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

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

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

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

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

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

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

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

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

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

SECTION 9. [NEW MATERIAL] EXCEPTIONS.--

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

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

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

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

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

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

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

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

(1) comply with federal or New Mexico law;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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