LFC Requester:	Felix Chavez

AGENCY BILL ANALYSIS - 2025 REGULAR SESSION

SECTION I: GENERAL INFORMATION

{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Date Prepared: February 25, 2025

Bill Number: HB 410

Check all that apply:

Original ___ Correction ___

Amendment ___ Substitute X

Sponsor: Rep. Linda Serrato

Short Title: Consumer Information and Data Protection Act

Agency Name and Code Number: 305 – New Mexico Department of Justice

Person Writing Analysis: AAG Jeff Dan Herrera/AAG Joshua Holst

Phone: 505-537-7676

Email: legisfir@nmag.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY25	**FY26**		

(Parenthesis ( ) indicate expenditure decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY25	**FY26**	**FY27**		

(Parenthesis ( ) indicate revenue decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY25	FY26	FY27	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total						

(Parenthesis ( ) Indicate Expenditure Decreases)

Duplicates/Conflicts with/Companion to/Relates to:
Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

This analysis is neither a formal Opinion nor an Advisory Letter issued by the New Mexico Department of Justice. This is a staff analysis in response to a committee or legislator's request. The analysis does not represent any official policy or legal position of the NM Department of Justice.

BILL SUMMARY

ORIGINAL

Synopsis: HB 410 would establish a broad consumer data protection law, with specific protections afforded to consumer health data.

Section 1: This section titles the new law, Sections 1 to 11 of this Act, as "Consumer Information and Data Protection Act."

Section 2: This section defines several terms used throughout the Act.

Section 3: This section provides several prohibitions relating to the use and dissemination of "consumer health data" for any person conducting business in New Mexico or producing products or services targeted to New Mexico residents. However, exempted from these prohibitions are several classes of persons and data, including nonprofit organizations, institutions of higher education, and persons and data that are regulated by federal laws bearing upon the use, maintenance, or dissemination of data.

The bill would prohibit covered persons from (1) providing consumer health data to an employee or contractor unless they are subject to a duty of confidentiality; (2) providing a "processor" (i.e., "a person who processes personal data on behalf of a controller," which is defined as a person who "determines the purpose and means of processing personal data") with access to consumer health data unless the processor complies with Section 6; (3) using a "geofence" to set a boundary within 1,750 feet of a mental health, reproductive, or sexual health facility in order to identifying, tracking, or collecting data from a consumer or sending a notification to a consumer regarding their health data; and (4) selling or offering to sell a consumer's health data without getting their consent.

Section 4: In lieu of a private right of action, the bill authorizes consumers to enforce their rights under the Act by notifying a controller of their intent to invoke their rights under the Act. A consumer may request to access, correct, delete, obtain, or opt out of the processing of their "personal data" for commercial purposes.

A controller must take one of several measures in response to a consumer's invocation of their rights, including responding to the request, declining to take action, and providing an appeals process for the consumer. In the event a consumer's appeal is denied, the consumer may submit a

complaint to the New Mexico Department of Justice (NMDOJ).

Section 5: This section imposes limitations and requirements on a controller's collection, processing, maintenance, and sale of personal data, including heightened protections for the processing of a child's personal data and the collection of a child's geolocation data.

Section 6: This section imposes on processors the duty to adhere to a controller's instructions and to assist a controller in meeting its obligations under the Act. Any contract executed between a controller and processor must detail the means by which the processor will meet this requirement.

Section 7: This section requires controllers to assess its processing activities of personal data, taking into account the benefits to a controller, a consumer, stakeholders, and the public and the risks relating to consumers' rights. The NMDOJ may issue a civil investigative demand and obtain such assessment, which is to be kept confidential and exempt from the New Mexico Inspection of Public Records Act.

Section 8: This section creates requirements to ensure a controller properly de-identifies a consumer's data, and exempts from the requirements of Section 4 a consumer's data that a cannot be associated with the consumer, is not used to recognize or respond to a consumer, and is not sold or disclosed to a third-party.

Section 9: This section clarifies that the Act shall not prevent a controller or processor from meeting its existing obligations, including its compliance with other laws and investigations, ability to prove or defend against legal claims, ability to transact with a consumer, ability to protect the life or safety of a person, ability to identify, protect against, or respond to illegal activity, and ability to engage in public or peer-reviewed research under certain privacy-oriented conditions.

The section further clarifies that a third-party's violation of the Act is not necessarily imputed to the controller or processor that disclosed personal data to the third-party, if the controller or processor had no actual knowledge of the intent to commit a violation.

The section states that it should not be construed as restricting a controller's or processor's ability to exercise the right of free speech.

Section 10: The NMDOJ would be empowered with investigating violations of the Act by means of a civil investigative demand.

Section 11: The NMDOJ is solely responsible for enforcing the Act, and may initiate an action for injunctive relief and civil penalties after providing thirty-day' written notice to the entity, after which time the entity must cure its violation and provide an express written statement of the cure.

The section clarifies that the Act should not be construed as creating a private right of action.

SUBSTITUTE

The proposed committee substitute (the "Substitute") of HB410 adds new sections from the original bill (the "Bill") concerning the obligations of large regulated entities, data obtained from

federal agencies, and severability.

Section 2: Section 2 of the Substitute adds new definitions relevant to new sections of the Bill added in the Substitute.

Section 3: Section 3 of the Substitute adds the scope of the Act, applying it to persons that conduct business in New Mexico and persons that produce products or services targeted to New Mexicans that in the previous calendar year either controlled or processed the data of at least 35,000 consumers or processed the personal data of at least 10,000 consumers and derived more than 20% of its gross revenue from the sale of personal data.

Section 4: Section 4 of the Substitute adds a subsection (6) requiring that a controller provides to a consumer an effective mechanism to revoke their consent that is at least as easy to use as the mechanism by which the consumer provided their consent.

Section 5: Section 5 of the Substitute adds that a consumer may designate an authorized agent that can act on the consumer's behalf to opt out of data processing for the purposes listed in Section 4.

Section 6: Section 6 of the Substitute imposes transparency requirements on controllers. It requires that data not be processed for purposes other than those disclosed and limits the collection of personal data to what is adequate for the purposes for which it is being collected. It also requires controllers to establish reasonable safeguards to protect the integrity of collected personal data. Additionally, it requires that controllers not discriminate against consumers for exercising their rights under the Act. This section then prohibits a controller from processing a consumer's sensitive personal data without first obtaining the consent of the consumer. It then imposes requirements on controllers to provide a privacy notice for consumers and lists the requirements for that notice. Subsection F then lays out specific purposes for which the processing of data for a known child is prohibited. Subsection G prohibits collecting geolocation data from a known child unless reasonably necessary for the feature or service in use and the controller provides an obvious signal to the child that the data is being collected for the duration.

Section 7: Section 7 of the Substitute imposes additional responsibilities on controllers. Subsection A imposes a duty of reasonable care to avoid heightened risk of harm to minor users using their service when the controller knows or willfully disregards that it has minor users. Subsection B prohibits the processing of the data of minors for specific prohibited purposes, and prohibits the use of any system design feature to significantly increase, sustain or extend any minor younger than the age of eighteen's use of such online service, without the consent of the minor or the minor's parents if the minor is under 13 years old. Subsection C prohibits collecting geolocation data from a known minor unless reasonably necessary for the feature or service in use and the controller provides an obvious signal to the minor that the data is being collected for the duration, and again requires obtaining the consent of the minor (or the minor's parents if the minor is under 13) before processing such data. Subsection E prohibits offering direct messaging to minors without readily accessible and easy to use safeguards (with some exceptions), and prohibits providing any consent mechanism designed to subvert or impair user autonomy.

Section 8: Section 8 of the Substitute imposes requirements on controllers to conduct a data assessment within one year of the Act taking effect consistent with Section 7 of the act that addresses purpose of the online service, the categories of minors' personal data that they collect, the purposes for which they collect that data, and any heightened risk of harm reasonably foreseeable as a result of offering the online service. Subsection B imposes requirements on

controllers review the data protection assessment as necessary, and to maintain the documentation of the assessment for the longer of 3 years or as long as the controller continues to offer its online service. Subsection E requires a controller to mitigate or eliminate any heightened risk of harm to minors if discovered in a data protection assessment. Subsection F exempts data protection assessments from IPRA.

Section 9: Section 9 of the Substitute reflects Section 6 of the Original.

Section 10: Section 10 of the Substitute reflects Section 7 of the Original.

Section 11: Section 11 of the Substitute reflects Section 8 of the Original.

Section 12: Section 12 of the Substitute reflects Section 9 of the Original.

Section 13: Section 13 of the Substitute provides certain rights regarding personal data to residents that use covered platforms. Subsection A allows covered residents to request that a platform disclose the categories of sensitive data they have collected and where they have collected it from, the purpose for collecting the data and third parties to whom the data was disclosed. Subsection B allows covered residents to request that covered platforms delete sensitive data they have collected on the consumer. Subsection C enables residents to exercise these rights at any time, and requires the covered platform to comply by making methods available to covered residents to submit a request for disclosure or deletion and disclose and deliver the required information to the resident within 30 days of the request. It further allows the platform to require authentication of the resident that is reasonable in light of the nature of the information requested. Subsection D enables the attorney general to enforce the provisions of the section, and gives the attorney general authority to investigate potential violations. Subsection E provides the attorney general a cause of action for which they may pray for injunctive relief and a penalty of $10,000 for each violation of the section.

Section 14: Subsection A prohibits the sharing or disclosure of data in the possession of a federal agency without the consent of the covered resident, except where done pursuant to a law lawfully enacted by the federal government. Subsection B provides that the federal government may not interfere with this Section without lawful preemption. Subsection C provides that the attorney general may investigate violations through civil investigative demands and bring a cause of action seeking injunctive relief and a $10,000 civil monetary penalty per violation.

Section 15: Section 15 of the Substitute reflects Section 10 of the Original.

Section 16: Section 16 of the Substitute reflects Section 11 of the Original.

Section 17: Section 17 provides for severability of the provisions of the Act. The Section explicitly requires that if a court finds one provision of the Act unconstitutional or preempted, the remaining provisions of the Act remain in effect.

FISCAL IMPLICATIONS
N/A

SIGNIFICANT ISSUES

Section 16
Section 16 expressly provides that the attorney general shall have the authority to enforce the Act. The Section creates a procedure for enforcement for all provisions other than Sections 13

and 14. The procedure in Section 16 requires the attorney general to provide entities a thirty-day period to cure any violations and make an express written statement that such violations have been cured. If violations continue, the attorney general may initiate an action to remedy the violation, including injunctive relief and a $10,000 civil penalty per violation. Section 14 additionally provides a cause of action for the attorney general—and identifies available remedies—relating to data in the possession of federal agencies.

Section 16(B), providing for the right of an entity in violation to cure, does not provide any specific oversight/compliance authority for the attorney general.

PERFORMANCE IMPLICATIONS

None noted.

ADMINISTRATIVE IMPLICATIONS

None noted.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

Conflict

HB307 (and SB420, which is substantially the same). HB307 would create the "Internet Privacy and Safety Act." HB307 pursues comparable goals to that of HB410—providing for greater privacy over personal data for consumers—but in ways that would conflict if both bills are passed. Most notably, HB307 requires an affirmative "opt-in" requirement. Covered entities are prohibited from collecting and processing personal data as a default setting, unless necessary to perform the service at issue. Whereas HB410 permits covered residents to request not to have data processed or for it to be deleted (an "opt-out" provision). Additionally, the fines for violation in HB410 are greater than that in HB307. HB307 requires the attorney general to promulgate rules for its enforcement. HB307 creates a private right of action whereas HB410 provides all enforcement power to the attorney general.

SB 420: The right to cure provisions for small businesses in SB 420 would be in conflict with the right to cure provisions in Section 16 of HB410.

SB309. SB309 potentially conflicts with HB410. SB309 requires that any public entity in the possession of global positioning system data concerning the location of a defendant on pretrial release shall share that data with a law enforcement officer upon request. HB410 provides that no person shall establish a geofence within 1,750 feet of a mental health care facility or reproductive health care facility. Additionally, data controllers are prohibited from collecting geolocation data on children (individuals under the age of 13). Whether the two bills are in conflict is a question of the definition of "person" under HB410. HB410 defines a "person" as "an individual, association, company, limited liability company, corporation partnership, sole proprietorship, trust or other legal entity." A court may find that a government body collecting data may fall under "other legal entity." Whether a court would find that the legislature intended to prohibit the provisions discussed in SB309 would be a question of statutory interpretation and is unclear without legal briefing on the matter.

The bill may overlap with the protections afforded under the Privacy Protection Act (PPA), NMSA 1978, §§ 57-12B-1 to -4, and the Data Breach Notification Act (DBNA), NMSA 1978, §§ 57-12C-1 to -12. To the extent a person's social security number may be considered "personal data" under the bill, there may be overlap with the PPA's prohibition against a business's dissemination of a person's social security number. Further, the bill's requirements may overlap with the DBNA's requirements to implement security measures for the maintenance of "personal

identifying information." See §§ 57-12C-4, -5.

TECHNICAL ISSUES
None noted.
OTHER SUBSTANTIVE ISSUES
None noted.
ALTERNATIVES
N/A
WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Status quo.

AMENDMENTS