FISCAL IMPACT REPORT

SPONSOR House Commerce and Economic Development Committee

LAST UPDATED

ORIGINAL DATE 3/8/25

BILL NUMBER CS/House Bill 410/HCEDCS/aHCEDC

SHORT TITLE Consumer Info & Data Protection Act

ANALYST Chavez

REVENUE*
(dollars in thousands)

Type	FY25	FY26	FY27	FY28	FY29	Recurring or Nonrecurring	Fund Affected
Fines and Forfeitures	No fiscal impact	$10.0 to $1,000.0	$10.0 to $1,000.0	$10.0 to $1,000.0	$10.0 to $1,000.0	Recurring	General Fund

Parentheses ( ) indicate revenue decreases.
*Amounts reflect most recent analysis of this legislation.

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT*
(dollars in thousands)

Agency/Program	FY25	FY26	FY27	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
NMAG	No fiscal impact	$131.8 to $527.2	$131.8 to $527.2	$263.6 to $1,054.4	Recurring	General Fund
Courts	No fiscal impact	Indeterminate but minimal	Indeterminate but minimal	Indeterminate but minimal	Recurring	General Fund
Total	No fiscal impact	$131.8 to $527.2	$131.8 to $527.2	$263.6 to $1,054.4	Recurring	General Fund

Parentheses ( ) indicate expenditure decreases.
*Amounts reflect most recent analysis of this legislation.

Conflicts with House Bill 307 and Senate Bills 309 and 420.

Sources of Information

LFC Files

Agency Analysis Received From
New Mexico Attorney General (NMAG)
Regulation and Licensing Department (RLD)

Agency Analysis was Solicited but Not Received From
Department of Finance and Administration (DFA)
Higher Education Department (HED)

Agency Declined to Respond
Department Of Information Technology (DoIT)
Office of Broadband Access and Expansion (OBAE)

SUMMARY

Synopsis of HCEDC amendment to House Bill 410

The House Commerce and Economic Development Committee (HCEDC) amendment to House Bill 410 replaces "and" with "or", changing the definition of "publicly available information" from meaning information that is lawfully made available through federal, state or local government records **and** a person has a reasonable basis to believe a consumer has lawfully made available to the general public to being information that is lawfully made available through federal, state or local government records **or** a person has a reasonable basis to believe a consumer has lawfully made available.

Synopsis of HCEDC Substitute for House Bill 410

The House Commerce and Economic Development Committee (HCEDC) substitute for House Bill 410 (HB410) enacts the Consumer Information and Data Protection Act, establishing new regulations for the collection, processing, and protection of personal data in New Mexico. HB410 would regulate businesses that conduct operations in New Mexico or offer products and services targeted to residents that in the previous calendar year which either controlled or processed the data of at least 35 thousand consumers or controlled or processed the personal data of at least 10 thousand consumers and derived more than 20 percent of its gross revenue from the sale of personal data. The regulation would prohibit these entities from providing employees or contractors access to consumer health data unless that individual is contractually or statutorily obligated to confidentiality. The bill restricts businesses from providing a processor (an entity that processes personal data on behalf of a business) with access to consumer health data and from selling or offering to sell the consumer's health data without first obtaining the consumer's consent. The bill would also restrict the use of geofencing (a virtual boundary created around a specific geographic area) from establishing a virtual boundary within 1,750 feet of any mental health facility or reproductive or sexual health facility for purposes relating to data or sending consumer notification regarding the consumer's health data.

Certain entities and data types are exempt from the bill's provisions, including government agencies, financial institutions subject to the Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.), and healthcare entities governed by HIPAA (Health Insurance Portability and Accountability Act). Additionally, nonprofit organizations and institutions of higher education are excluded from the bill's requirements.

HB410 enumerates consumer rights and responsibilities of the controller (entities that determine the purpose and means of processing personal data) and processor. HB410 would allow a consumer or the consumer's parents if they are underage to exercise the right to:

- Confirm whether the business has access to and is processing the consumer's personal data;
- Correct inaccuracies in the consumer's data;
- Delete personal data provided by or obtained about the consumer;
- Obtain a copy, in a portable and readily usable format, of the consumer's personal data that allows the consumer to transmit the data to another business without hindrance, in an automated fashion; and
- Opt out of personal data processing that uses that data in matters that produce legal or similarly significant effects concerning the consumer.

The bill would establish that businesses would have to provide secure and reliable means to allow the consumer to exercise the rights prescribed in the bill and describe those means to the consumer in the business's privacy notice. This section also adds the case of when a consumer is subject to guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise such rights on the consumer's behalf.

HB410 outlines how controllers must handle consumer requests regarding their personal data. Controllers must respond within 45 days, though they can extend this once for another 45 days, if necessary, as long as they notify the consumer within the initial period. If a request is denied, the consumer must be informed within 45 days and given appeal instructions. Consumers can make two free requests per year, but if requests are excessive or repetitive, controllers may charge a reasonable fee or refuse them. Controllers must verify the identity of the consumer before acting on a request. If a controller received a consumer's data from another source, it could comply with a deletion request by either keeping a minimal record of the request to prevent future use or opting the consumer out of data processing, except in cases where the law allows exceptions. Controllers would also have to provide an effective mechanism for consumers to easily withdraw their consent for their data to be processed. The mechanism to revoke consent should be at least as simple as the way the consumer gave their consent in the first place. After the consent is revoked, the controller must stop processing the consumer's data as soon as possible, and no later than 15 days after receiving the request to revoke consent.

If a controller denies a consumer's request regarding their personal data, it must provide an appeal process that is easy to find and like the original request process. The business has 60 days to respond to an appeal with a written explanation of its decision. If the appeal is denied, the business must inform the consumer of a way to file a complaint with the attorney general, either through an online system or another method.

HB410 would also allow a consumer to appoint another person (an authorized agent) to act on their behalf in opting out of the processing of their personal data for certain purposes specified in HB410. The consumer can designate the agent through various methods, such as using an internet link, browser setting, or other technology. The controller must honor the opt-out request from the authorized agent if they can reasonably verify both the consumer's identity and the agent's authority to act on the consumer's behalf.

HB410 outlines various responsibilities for controllers handling personal data. These include limiting data collection to what is necessary, ensuring security, and not processing data in ways that violate laws or discrimination regulations. Controllers must also provide clear privacy notices, disclose data sales or targeted advertising, and allow consumers to exercise their rights, including opting out of data processing. Additionally, controllers are prohibited from collecting or processing sensitive data from children without consent and must comply with the Children's Online Privacy Protection Act, a federal regulation. The bill also 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. Any contract that limits consumer rights is considered void.

The bill also imposes additional responsibilities on controllers. HB410 imposes a duty of reasonable care to avoid any heightened risk of harm to suers that are minors when the controller knows or willfully disregards that it has these users. The bill prohibits controllers, who know or

willfully disregard that it has users that are minors, from processing personal data of any of the users for the purposes of targeted advertising, any sale of personal data or using profiling for fully automated decisions that affect access to essential services like finance, housing, or healthcare, unless necessary for the service provided or compatible with the original purpose, and only for as long as needed. Controllers are further prohibited from using a system design feature that significantly increases, sustains or extends the use of an online service, product or feature for users younger than 18 years of age unless the service or application is used by and under the direction of an educational entity or with the consent of the minor or the minor's parents if the minor is under 13 years old. Controllers would also not be allowed to provide users, under the age of 18, with any consent mechanism that is designed to subvert or impair user autonomy, decision-making, or choice and from offering direct messaging to minors without readily accessible and easy to use safeguards.

HB410 would also call for controllers, who have consumers that they know are minors, to conduct a data protection assessment for any online service, product or feature on or one year after the effective date of HB410. The data protection system would be consistent with the requirements in the previous paragraph of this analysis. The data protection system would have to address:

- The purpose of the online service, product or feature,
- The categories of minors' personal data that the online service, product or feature processes,
- The purposes for which the controller processes minors' personal data, and
- Any heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product or feature to minors.

Controllers would also have to review the data protection assessment as necessary and maintain documentation concerning the data protection for the longer of three years beginning on the date data processing ceases or as long as the controller offers the online service, product or feature. If a data protection assessment discovers a heightened risk of harm to minors, the controller must establish and implement a plan to mitigate or eliminate that risk.

If controllers are contracting processors, the bill outlines that they must follow the controller's instructions and assist in fulfilling the obligations of the bill. A contract between the controller and processor must define processing procedures, confidentiality, data retention, and cooperation for assessments. If the processor uses subcontractors, it must ensure subcontractors comply with these obligations. Both the controller and processor remain liable for their roles in data processing.

HB410 requires controllers to also conduct data protection assessments for certain data processing activities, including targeted advertising, the sale of personal data, profiling that may harm consumers, processing sensitive data, and activities with heightened risks to consumers. These assessments must evaluate the potential benefits and risks, considering safeguards and factors like de-identified data (data that cannot be reasonably used to identify an individual) and consumer expectations. New Mexico Attorney General (NMAG) can request these assessments for investigation purposes, and they will remain confidential. Data protection assessments can cover similar processing operations and may align with assessments for other laws, provided they meet comparable requirements. These requirements apply to new processing activities and are not retroactive.

The bill outlines requirements for controllers handling de-identified data. Controllers must take reasonable measures to ensure the data cannot be linked to individuals, commit to not re-identifying it, and contractually require recipients to comply with HB410. HB410 does not mandate the re-identification of de-identified or pseudonymous data or the maintenance of identifiable data for associating consumer requests. Controllers are not required to comply with consumer rights requests if associating the request with personal data is not feasible, is excessively burdensome, controller does not use personal data to recognize or respond to a specific consumer, or the controller does not sell or share the personal data. Pseudonymous data is exempt from consumer rights requests if it is kept separately and protected by controls. Controllers must also oversee compliance and address breaches when disclosing pseudonymous or de-identified data.

HB410 allows controllers and processors to process data for legal compliance, law enforcement cooperation, legal claims, consumer safety, and internal research.

HB410 also provides regulation on data in the possession of federal agencies. The bill would stipulate that no person can share or disclose a covered resident's (natural person who lives in or is domiciled in New Mexico) sensitive data held by a federal agency without the resident's consent, unless required by a law passed by the United States Congress. The bill further allows the covered resident or NMAG to request a third party, who receives sensitive data from the federal government without the authorization of federal law, to delete the information in its possession and disclose the source form which the information came from. NMAG would be able to intervene as a matter of right in any action seeking determination as to whether the requested disclosure is compliant. NMAG is also empowered to issue a civil investigation demand whenever NMAG has reasonable cause that an entity does not comply with the regulations on data in the possession of federal agencies.

HB410 grants exclusive enforcement authority to NMAG, who may issue civil investigative demands and seek civil penalties of up to $10 thousand per violation and may recover litigation fees. Prior to taking enforcement action, NMAG must provide businesses with 30-day notice to cure any alleged violations. The bill does not create a private right of action, meaning consumers cannot sue businesses directly for violations, but instead must rely on state enforcement. HB410 includes a severability clause.

This bill does not contain an effective date and, as a result, would go into effect 90 days after the Legislature adjourns if enacted, or June 20, 2025.

FISCAL IMPLICATIONS

HB410 would impose a financial obligation on the private entities required to develop methods and procedures to adhere to the regulations in HB410, like updating privacy notices to adhere to the mandated disclosures and the data protection assessments. Controllers and processors would more than likely have negotiations go longer as the bill stipulates both parties, when applicable, work together to adhere to the various disclosures and data provisions in HB410 that could cause conflict. The bill provides provisions that lessen the burden on private companies, however, because the bill explains that data provisions must be done in a way that is feasible and not excessively burdensome.

HB410 grants enforcement authority to NMAG, which can seek civil penalties of up to $10

thousand per violation and may recover litigation fees. Without data to inform an estimate on how many violations could occur, the revenue impact is based on one to 100 violations a year netting $10 thousand to $1 million. This is subject to how well NMAG can develop procedures to identify violations and how well it can prosecute the identified violations. HB410 does not provide additional funding to NMAG to identify and prosecute the violations of the act. Because of the lack of additional funding, NMAG could need additional resources to properly prosecute. NMAG could need an additional 1 to 4 FTE paid at the average salary in the Legal Services Program, the program related to the bill, of $131.8 thousand a year for an estimated operating expense impact of $131.8 to $527.2 thousand per year.

Because the bill would not create a private right of action and instead relies on state or NMAG for enforcement, HB410 is unlikely to financially impact the courts. The bill provides for the consumer to bring complaints against a company to NMAG, and some disputes may be resolved between the private entities to begin with.

SIGNIFICANT ISSUES

NMAG provides the following:

> 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.

The Higher Education Department (HED) explains in analysis for the original bill that HB410 offers protections for personal and sensitive information beyond commercial or employment situations, benefiting higher education students, faculty, staff, and HED personnel.

HED notes in analysis for the original bill the following about how higher education institutions (HEIs) work with third parties under the restrictions of federal Health Insurance Portability and Accountability Act (HIPAA) protecting patients' health information and the federal Family Educational Rights and Privacy Act (FERPA) protecting student information:

> HB410 speaks about controllers and processors working with third parties. HED and HEIs may share information with third parties, specifically third parties who are not state agencies or HEIs. If they share FERPA- or HIPAA-protected data, then … those data will remain protected by their respective laws, so HB410 does not need to provide further protections. But HED or HEIs may share other information that is not exempted from HB410, and it is unclear how HB410's protections apply once a third party who is not exempted as a group receives that data.

The Regulation and Licensing Department (RLD) provides the following analysis on the original

version of the bill:

- HB410 defines "child" as a person under the age of 13. Both the Children's Code and the Criminal Code define "child" as a person who is less than 18 years old. See §32A-1-4(C), NMSA 1978. See also §30-6-1(A)(1), NMSA 1978. If the intent is to have a particular class of children covered or exempt from the act, then it may be appropriate to include additional qualifying language explaining the distinction between how the term "child" is used in other sections of current law and the significantly lower age threshold specified in HB410.
- HB410 defines "biometric data" as "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. Biometric data does not include (1) a digital or physical photograph; (2) an audio or video recording; (3) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual."

The Data Breach Notification Act defines "biometric data" as "a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account." §57-12(C)-2, NMSA 1978. "Personal identifying information" in the Data Breach Notification Act, §§57-12C-2 to -12, NMSA 1978, includes biometric data as well as and individuals first or first initial and last name in combination with a social security number and/or driver's license number and/or government-issued identification number and/or account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial record.

"Biometric identifying information" is also defined as "physical characteristics used in verifying the identity of an individual, including photographs, fingerprint impressions and palm print impressions." §29-3-8, NMSA 1978 (2019). "Biometric data" can also include deoxyribonucleic acid (DNA).

"Biometric data means data, such as finger, voice, retina or iris prints or deoxyribonucleic acid, that capture, represent or enable the reproduction of unique physical attributes of a person." §30-16- 24.1, NMSA 1978.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

NMAG provides the following:

Conflict

House Bill 307 (HB307) (and Senate Bill 420 (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.

SB420: The right to cure provisions for small businesses in SB420 would be in conflict with the right to cure provisions in Section 16 of HB410.

Senate Bill 309 (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.

OTHER SUBSTANTIVE ISSUES

NMAG provides the following:

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.

HED reports in analysis for the original bill:

2022 House Joint Resolution 8 proposed to amend the Constitution of New Mexico to create an Office of Consumer Affairs to promote and protect the interests of the consumers of New Mexico. This joint resolution was postponed indefinitely. This office could have overseen consumer information and data similar to what we see in HB410.

FC/hj/sgs