epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

March 4, 2025

The Honorable Joseph Cervantes, Chair
Senate Tax, Business & Transportation Committee
New Mexico Legislature
490 Old Santa Fe Trail
Santa Fe, NM 8750

Dear Chair Cervantes, Vice Chair Maestas, and Members of the Committee:

EPIC writes in support of SB 420, the Community Privacy & Safety Act. For more than two decades, powerful tech companies have been allowed to set the terms of our online interactions. Without any meaningful restrictions on their business practices, they have built systems that invade our private lives, spy on our families, and gather the most intimate details about us for profit. But it does not have to be this way – we can have a strong technology sector while protecting personal privacy.

The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC has long advocated for comprehensive privacy laws at both the state and federal level.[2]

SB 420 builds on existing state privacy laws already enacted in nineteen states, while incorporating important provisions to provide New Mexicans with the protections they need to stay safe online.[3] Key provisions of SB 420 include:

- **Data minimization:** SB 420 establishes limits on the unfettered use of personal data by setting a baseline requirement that entities only collect, use, and transfer data that is necessary to provide the online feature, product or service with which the consumer is actively and knowingly engaged.

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] *See* e.g. Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security: Hearing before the Subcomm. on Consumer Protection & Comm. of the H. Comm. on Energy & Comm., 117th Cong. (2022) (testimony of Caitriona Fitzgerald, Deputy Director, EPIC), https://epic.org/wp-content/uploads/2022/06/Testimony_Fitzgerald_CPC_2022.06.14.pdf.
[3] *See* EPIC and U.S. PIRG Education Fund, *The State of Privacy 2025: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better* (Jan. 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-PIRG-State-of-Privacy-2025.pdf.

- **Strong protections for sensitive data:** SB 420 sets heightened protections for sensitive data (i.e., biometrics, location, health data) such that it cannot be used for advertising purposes.

- **Preventing discrimination:** SB 420 extends civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, condition related to pregnancy, or disability.

- **Requires "privacy by default:**" SB 420 requires that entities set default privacy settings to the highest level of privacy by default and establish reasonable data security practices.

- **Protections for children and teens:** SB 420 requires that when an entity knows a consumer is under 18 years of age, they must establish default settings that 1) disable contact by unknown users unless the minor first initiates the contact; 2) disables notifications between 10 PM and 6 AM; and 3) use a privacy-protective feed.

- **Strong enforcement mechanisms:** By including a private right of action, SB 420 gives consumers the same strong enforcement options for privacy violations that they have for other violations of their rights as consumers, including the right to sue for violations and Attorney General enforcement.

- **Rulemaking authority.** Attorney General rulemaking authority in a privacy law is essential to allow the law to keep pace with constantly evolving technologies and to effectively implement the technical requirements under the bill.

In my testimony I will discuss why it is so critical that New Mexico pass a privacy law and go into detail on a couple of key concepts that are crucial in any strong privacy bill.

Data Abuse is Hitting Americans' Wallets

Companies should not have a limitless ability to decide how much personal data to collect. Unfortunately, this is what all state laws — other than California's and Maryland's — allow. Most existing state privacy laws only limit collection to what is reasonably necessary for "the purposes for which such data is processed, *as disclosed to the consumer*," meaning businesses can collect data for whatever purposes they want, as long as they state that purpose in their privacy policies.[4] This reinforces the failed status quo of "notice and choice" — businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. The focus on notice has led to longer and more complicated privacy policies that users do not read and could not change even if they did.

Advertisers and data brokers track our every click, and our data is used against us in ways that harm our wallets, opportunities, and rights. At a time when policymakers are concerned about

[4] *See id.*

cost-of-living issues for their constituents, the impact of mass data collection and abuse on those costs cannot be ignored. A few examples of these harms include:

1. **Increased insurance premiums.** Last month, the Texas Attorney General sued insurance giant Allstate for unlawfully collecting, using, and selling data about the location and movement of Texans' cell phones through secretly embedded software in mobile apps such as Life360. Paxton alleged that Allstate and other insurers then used the covertly obtained data to justify raising Texans' insurance rates.[5]

2. **Increased pricing on consumer goods**. Last month, the Federal Trade Commission released initial findings from a study on surveillance pricing, and found that "retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage."[6] Grocery stores are adopting electronic shelf labels to use "dynamic" pricing "in which the price of basic household goods could surge based on the time of day, the weather, or other transitory events."[7]

3. **Targeted advertisements can be predatory and harmful.** Targeted ads can be predatory and harmful, using people's online behavioral data to reach vulnerable consumers who meet specific parameters. People searching terms like "need money help" on Google have been served ads for predatory loans with staggering interest rates of over 1,700%.[8] An online casino targeted ads to problem gamblers, offering them free spins on its site.[9] A precious metals scheme used Facebook users' ages and political affiliations to target ads to get users to spend their retirement savings on grossly overpriced gold and silver coins.[10]

---

[5] Press Release, Att'y Gen. of Texas, *Att'y Gen. Ken Paxton Sues All-state and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Cos.* (Jan 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

[6] Press Release, Fed. Trade Comm'n, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[7] Letter from Sen. Elizabeth Warren to Rodney McMullen, CEO and Chairman, The Kroger Co. (Aug. 25, 2024), https://www.warren.senate.gov/imo/media/doc/warren_casey_letter_to_kroger_re_electronic_shelving_and_price_gouging.pdf.

[8] Shanti Das, *Google Profiting from 'Predatory' Loan Adverts Promising Instant Cash*, The Guardian (Mar. 13, 2022), https://www.theguardian.com/technology/2022/mar/13/google-profiting-from-predatory-loan-adverts-promising-instant-cash.

[9] Rob Davies, *Online Casino Advert Banned for Targeting Problem Gamblers*, The Guardian (Oct. 9, 2019), https://www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling.

[10] Jeremy B. Merrill, *How Facebook Fueled a Precious-Metal Scheme Targeting Older Conservatives,* Quartz (Nov. 19, 2019), https://www.yahoo.com/video/facebook-fueled-precious-metal-scheme-110044886.html.

Small businesses are harmed by these systems as well. For years, they've been told that success hinges on pouring money into online behavioral advertising, controlled by a handful of tech giants. They enter bidding wars against corporate behemoths. This isn't a level playing field. It's a digital black hole—swallowing resources and crushing entrepreneurial spirit, all to facilitate targeted advertising that is of dubious efficacy.

Data Minimization and Strong Enforcement: Two Keys to a Strong Privacy Law

Data Minimization

SB 420 relies on a concept that has long been a pillar of privacy protection in order to force changes to harmful data abuse: data minimization.

When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose and duration necessary to provide the goods or services that they requested. For example, a consumer using a map application to obtain directions would not reasonably expect that their precise location data would be disclosed to third parties and combined with other data to profile them. And indeed, providing this service does not require selling, sharing, processing, or storing consumer data for unrelated secondary purposes. Yet these business practices are widespread. Nearly every online interaction can be tracked and cataloged to build and enhance detailed profiles and retarget consumers. Even offline, credit card purchases, physical movements, and "smart" devices in homes create countless data points that are logged and tracked without consumer awareness or control.

SB 420 sets a baseline requirement that entities only collect, use, and transfer data that is necessary to provide the online feature, product or service with which the consumer is actively and knowingly engaged (or pursuant to certain enumerated purposes). This standard better aligns business practices with what consumers expect.

Data minimization is essential for both consumers and businesses. Data minimization principles provide much-needed standards for data security, access, and accountability, assign responsibilities with respect to user data, and restrict data collection and use. Indeed, a data minimization rule can provide clear guidance to businesses when designing and implementing systems for data collection, storage, use, and transfer. Data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

Data minimization is not a new concept. Privacy laws dating back to the 1970s have recognized and applied this concept. The Privacy Act of 1974, a landmark privacy law regulating the personal data practices of federal agencies, requires data minimization. Each agency that collects personal data shall "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[11]

[11] 5 U.S.C. § 552a (e)(1).

The Maryland Online Data Privacy Act, enacted last year, and the California Consumer Privacy Act also include provisions requiring a form of data minimization. The key with a data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for and discloses in its privacy policy.

Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data.

Enforcement is Critical

Robust enforcement is critical to effective privacy protection. Strong enforcement by state government via Attorney General authority or the creation of a state privacy agency is a very important piece to include in a strong privacy law, and funds should be appropriated to ensure the Attorney General can meaningfully enforce the law.

But while government enforcement is essential, the scope of data collection online is simply too vast for one entity to regulate. Individuals and groups of individuals who use these online services are in a good position to identify privacy issues and bring actions to vindicate their interests. These cases preserve the state's resources, and statutory damages ensure that companies will face real consequences if they violate the law.

The inclusion of a private right of action is the most important tool the Legislature can give to their constituents to protect their privacy. A private right of action would impose enforceable legal obligations on companies. As Northeastern University School of Law Professor Woody Hartzog recently wrote with regard to a private right of action in the Illinois biometric privacy law:

> So far, only private causes of action seem capable of meaningfully deterring companies from engaging in practices with biometrics based on business models that inevitably lead to unacceptable abuses. Regulators are more predictable than plaintiffs and are vulnerable to political pressure. Facebook's share price actually rose 2 percent after the FTC announced its historic $5 billion fine for the social media company's privacy lapses in the Cambridge Analytica debacle. Meanwhile, Clearview AI specifically cited BIPA as the reason it is no longer pursuing non-government contracts. On top of that, Clearview AI is being sued by the ACLU for violating BIPA by creating faceprints of people without their consent. […] In general, businesses have opposed private causes of action more than other proposed privacy rules, short of an outright ban.[12]

[12] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, AI Now Institute (2020), https://ainowinstitute.org/regulatingbiometrics-hartzog.pdf

The ACLU's suit against facial recognition company Clearview AI settled, with Clearview agreeing not to sell its face surveillance system to any private company in the United States.[13] Private rights of action are extremely effective in ensuring that the rights in privacy laws are meaningful.

Many privacy laws include a private right of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations. Consumers should be able to seek redress for privacy violations the same way they would for other violations of their consumer rights. We encourage the Committee to retain this provision.

* * *

Privacy is a fundamental right, and it is time for business practices to reflect that reality. Self-regulation is clearly not working, and since Congress has still been unable to enact comprehensive privacy protections despite years of discussion on the topic, state legislatures must act. The New Mexico Legislature has an opportunity this session to provide real privacy protections for New Mexicans.

I am happy to be a resource to the Committee as it navigates this complex topic and can be reached at fitzgerald@epic.org.

Sincerely,

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Deputy Director

/s/ *Kara Williams*
Kara Williams
EPIC Law Fellow

[13] Ryan Mac and Kashmir Hill, *Clearview AI Settles Suit and Agrees to Limit Sales of Facial Recognition Database*, N.Y. Times (May 9, 2022), https://www.nytimes.com/2022/05/09/technology/clearview-ai-suit.html.