ACLU Colorado

2025 Report

Colorado Tech and Privacy Legislation

Gaps, Constitutional Challenges, and National Implications

Introduction

The increasing integration of digital technologies and artificial intelligence (AI) into everyday life has prompted many states, including Colorado, to take proactive measures to regulate personal data collection, biometric identifiers, algorithmic decision making, and strengthen consumer safety across various forms of tech. From AI-based hiring platforms to facial recognition, **the risks of digital surveillance are no longer theoretical.** Despite the state's legislative momentum, several recently passed laws contain significant gaps related to scope and enforcement. This report examines the Colorado Privacy Act (CPA), House Bill 24-1130 (expansion of biometric identifiers protections), Senate Bill 24-205 (high risk AI decisions), Senate Bill 22-113 (public sector use of facial recognition), and recent proposals regarding age verification on social media. Drawing on relevant federal case law and national regulatory models, the report provides practical recommendations to ensure future laws are enforceable and constitutionally sound, while also balancing innovation and individual rights.

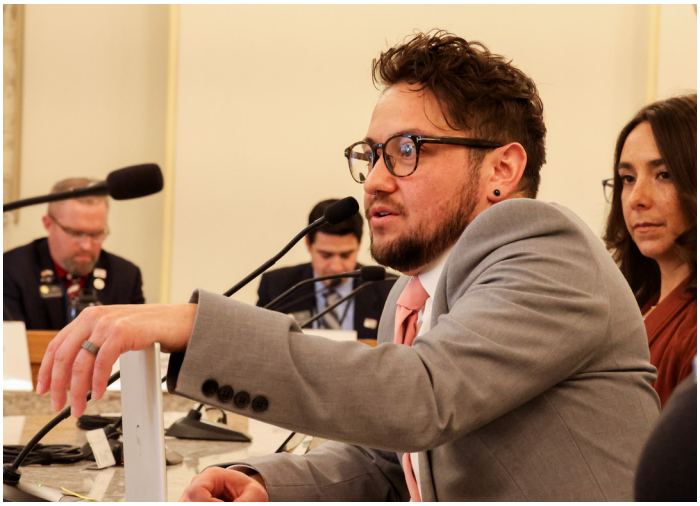
The Colorado Privacy Act and HB24-1130: Private Sector Data Privacy and Expansion of Biometric Protections

Summary of the CPA and HB24-1130

The Colorado Privacy Act (CPA), effective July 1, 2023, grants Colorado's consumers the right to access, correct, delete, and opt out of the processing of their personal data. House Bill 24-1130, effective July 1, 2025, expands the CPA to more robustly protect biometric identifiers such as retina scans, fingerprints, voiceprints, and facial recognition data. The amendment mandates affirmative consent for collection of biometric data, limits retention periods, requires deletion protocols, and prohibits the sale and purchase of biometric identifiers (Colo. Rev. Stat. § 6-1-1301 et seq.).

Gaps and Implementation Issues

While the expansion is a move in the right direction, a critical shortcoming of the CPA remains: the absence of an express private right of action. Enforcement authority resides solely



Anaya Robinson, ACLU of Colorado public policy director, testifies in support of HB24-1130 in February 2024.

with the Colorado Attorney General and district attorneys, limiting consumers' ability to seek redress. This contrasts with the Illinois Biometric Information Privacy Act (BIPA), for example, under which private plaintiffs have initiated hundreds of enforcement actions. In *Rosenbach v. Six Flags Ent. Corp.* (2019), the Illinois Supreme Court held that individuals need not show actual harm to sue under BIPA. This policy provides a model for strong enforcement.

The CPA also leaves gaps in data protection outside of consumer-controller relationships. Legislating new privacy statutes that cover other arenas, including public school, employment and labor, and the government sector as a whole, is imperative to ensure that vulnerable data across all areas of Coloradans' lives is protected. Furthermore, many industries and business types are exempt from the CPA and are instead subject only to federal laws. But federal laws may be weakened, inadequately enforced, or eliminated. The CPA should be further amended to increase protection at the state level so that consumers are not reliant on federal action.

Federal Caselaw Implications

In *Carpenter v. United States* (2018), the U.S. Supreme Court held that historic cellphone location data is protected under the Fourth Amendment, setting a precedent that biometric and other sensitive digital state may also warrant constitutional safeguards. The Court recognized that technological advances create novel privacy threats that existing legal frameworks must accommodate. Case law like this is crucial in bridging the gap left in the CPA by the exemption of public entities.

Colorado SB24-205: AI Regulation and Delay in Implementation

Summary of SB24-205

SB24-205, passed in 2024, is one of the nation's most ambitious efforts to regulate AI. It targets developers and deployers of "high risk" AI systems — defined as those that significantly affect decisions regarding employment, education, financial services, and healthcare. The law mandates algorithmic impact assessments, risk management plans, and consumer disclosures of AI use. It is set to take effect February 1, 2026, but there is a push from big tech and venture capital firms to delay implementation an additional year, or repeal the law altogether.

The statute's vague definitions — such as what constitutes "significant impact" — may also burden developers with uncertainty. Without clearer guidance or rules for risk evaluation, compliance efforts may be delayed or misapplied. The rebuttable presumptions and affirmative defenses that exist in the law, which are granted to companies who do the bare minimum for compliance, make it extremely hard for consumers to access appropriate recourse when discriminated against. Both should be repealed to allow for meaningful enforcement. When discriminatory harm occurs, we must protect the people, not the entities perpetrating the harm.

National and Legal Context

Federal AI legislation remains relatively static, though there have been attempts to both create regulation on the federal level and to preempt states' regulations and impose a moratorium on further regulation. The Blueprint for an AI Bill of Rights (2022), American Data Privacy and Protection Act (ADPPA), and the National Institute of Standards and Technology's (NIST) AI Risk Management Framework offer soft-law models. SB24-205's requirements echo procedural protections under the Fair Credit Reporting Act (FCRA). In *Spokeo, Inc. v. Robins* (2016), the U.S. Supreme Court emphasized the necessity of concrete harm for standing, suggesting that AI regulation must ensure both procedural transparency and substantive fairness. While federal law remains stalled, states must continue forward to ensure appropriate regulation in this fast-paced industry.

Colorado SB22-113: Public Sector Use of Facial Recognition

Summary of the Bill

SB22-113, enacted in 2022, regulates the use of facial recognition services by government agencies. It requires annual transparency reports, pre-use accountability reports, and prohibits law enforcement from conducting continuous real-time surveillance in public spaces without a warrant. The bill also prohibited K-12 public schools from using facial recognition services, unless grandfathered in, until July 1, 2025. SB25-143, enacted in 2025, put limits on K-12 schools' use of facial recognition services, prior to the repeal of the prohibition, to ensure guardrails are maintained in the future. Schools must gain consent before collecting biometric identifiers and may only use facial recognition surveillance on school grounds when there is a legitimate safety risk present.

As of 2024, only **15 states have regulated the use of facial recognition technology.**

Source: Tech Policy Press

Gaps in Enforcement and Oversight

Despite these provisions, the law lacks meaningful enforcement mechanisms. There is no express private right of action and penalties for violations are largely unclear or non-existent. The law permits ongoing data sharing with federal agencies, raising concerns about mission creep and surveillance overreach. At a time when Colorado purports to stand strong in protecting our most vulnerable, statutes that permit the sharing of sensitive data with an increasingly authoritarian government have no place in our state.

Constitutional Framework

This statute implicates both First and Fourth Amendment concerns. As seen in *Carpenter v. United States* (2018), persistent surveillance using digital tools may require warrants. Overly broad use of facial recognition risks infringing free association rights, as recognized in *NAACP v. Alabama* (1958). Greater limitations on interagency sharing and defined data retention limits are essential to preserving constitutional protections and should be amended into the statute to prevent unintended harm to civil liberties. Ultimately, prohibiting the use of these technologies without a judicial warrant or court order, especially within the realm of law enforcement, is the best approach to ensuring the preservation of constitutional rights.

Age Verification and Protections for Social Media and Constitutional Limits

Proposed Legislation

Over the past several years, lawmakers in Colorado and across the country have been considering age verification and user removal mandates for social media platforms. These mandates would require social media platforms to authenticate users via government-issued identification or biometric scans such as facial recognition or fingerprint verification and remove users who have violated the platforms' government-mandated policies. These proposals aim to shield minors from harmful content and limit their exposure to addictive digital features. Verification methods may include scanning a driver's license, submitting biometric identifiers, or using facial analysis to estimate age. While such mechanisms are intended to enhance child safety, they raise significant privacy and security concerns — particularly regarding the handling, storage, and potential misuse of sensitive personal data.

As of July 2025, **25 states have laws mandating some form of age verification** before accessing certain kinds of online content.

Source: Free Speech Coalition

Biometric Verification and Privacy Implications

Biometric verification refers to the use of unique biological, physical, or behavioral traits to authenticate a person's age. These traits can include facial geometry, voiceprints, search and browsing history, or hand geometry. Such methods are increasingly being employed due to their automation potential. However, they are also irrevocable: unlike passwords, biometric traits cannot be changed if compromised. The collection of such data introduces substantial risks, including unauthorized surveillance, data breaches, and secondary uses without consent. Data controllers must ensure robust security measures, yet recent breaches in both private and government systems demonstrate ongoing vulnerabilities. But recent examples of large-scale breaches, like the 2019 breach of the U.S. Customs and Border Protection database, which exposed traveler facial images, highlight the high stakes of biometric data misuse.

The implications for minors are even more severe. Requiring children or their guardians to upload government IDs or submit facial scans may deter engagement with lawful online services, particularly in marginalized communities. Moreover, storage of such data — whether by platforms or third-party verifiers — poses long-term surveillance and identity theft risks.

Furthermore, age verification processes directly conflict with the CPA. A controller may not deny access to goods or services, or limit such access that others would receive if an individual chooses not to share their sensitive data. Age verification policies that rely on biometric verification or government-issued identification would conflict with existing state law.

Constitutional Issues

These proposed laws raise serious First Amendment concerns, on top of their threats to privacy. Case law shows that minors hold free speech rights, and that anonymity is a protected condition of free expression. In *Brown v. Entertainment Merchants Association* (2011), the U.S. Supreme Court invalidated a California law that sought to restrict minors' access to violent video games, affirming that minors possess First Amendment rights. In *Doe v. Reed* (2010) and *NAACP v. Alabama* (1958), the Court reinforced the importance of anonymity for free expression, particularly when engaging in politically or socially sensitive speech.

Plus, courts have recently blocked similar age verification laws in *NetChoice v. Griffin* (E.D. Ark. 2023) and *NetChoice v. Bonta* (N.D. Cal. 2024), finding that age verification imposes burdens on free speech and anonymity disproportionate to the state's objectives. These cases highlight that even well-intentioned efforts to protect minors must pass strict scrutiny, requiring that laws be narrowly tailored and employ the least restrictive means to achieve their goal.

Beyond age verification, there are constitutional problems related to the removal of users for the violation of certain platform policies. Legislation that seeks to require speech platforms to remove users for policy violations has been struck down by the Court before. In *Packingham v. North Carolina* (2017), the U.S. Supreme Court unanimously struck down a North Carolina law that banned individuals convicted of sex offenses from social media platforms. The decision states that foreclosing access to social media would prevent users from engaging in the legitimate exercise of their First Amendment rights.

National Landscape

Over a dozen states have introduced or enacted age verification laws, reflecting growing bipartisan concern over youth mental health and online safety. However, most of these laws face immediate legal challenges due to constitutional infirmities. Civil liberties advocates argue that less invasive alternatives — such as opt-in parental controls, algorithmic transparency, and default privacy settings — can achieve the same goals without sacrificing individual rights. The continued scrutiny of these laws underscores the need for careful legislative drafting that respects both child welfare and constitutional guarantees.

Principles for Tech Regulation Without Infringing on Civil Liberties

Transparency and Procedural Safeguards

Laws should mandate clear consumer disclosures, right-to-explanation for AI outcomes, and fair appeals processes. These standards are consistent with the European Union's General Data Protection Regulation best practice and the emerging federal consensus as seen in Federal Trade Commission rulemaking efforts.

Narrow Tailoring and Least Restrictive Means

Any restriction on data practices or access to content must serve a compelling state interest and use the least restrictive means to meet strict scrutiny in First Amendment complaints. Legislation should have narrow solutions to focus on problems, rather than issuing broad restrictions on speech platforms.

Protecting Anonymity and Consent

Digital laws must preserve anonymity, especially in contexts involving speech or

political activity. Consent mechanisms should favor opt-in, rather than default opt-out, schemes. The decision in *NAACP v. Alabama* (1958) underscores how anonymity can be essential for participation in democratic processes.

Federal-State Harmonization

To avoid confusion and promote compliance, Colorado should align with federal norms where possible, and work with other states to ensure similar statutes across state lines while waiting for reasonable federal action. A national privacy baseline — augmented by robust state laws — would enhance protection while minimizing regulatory complexity. Bills seeking to preempt state laws — which are often created because of the absence of federal action — should be fought. Without substantial and meaningful federal law in this area, we will be left with no ways to regulate this industry or protect against unencumbered collection, use, retention, and commodification of our most sensitive and vulnerable data.

Conclusion and Recommendations

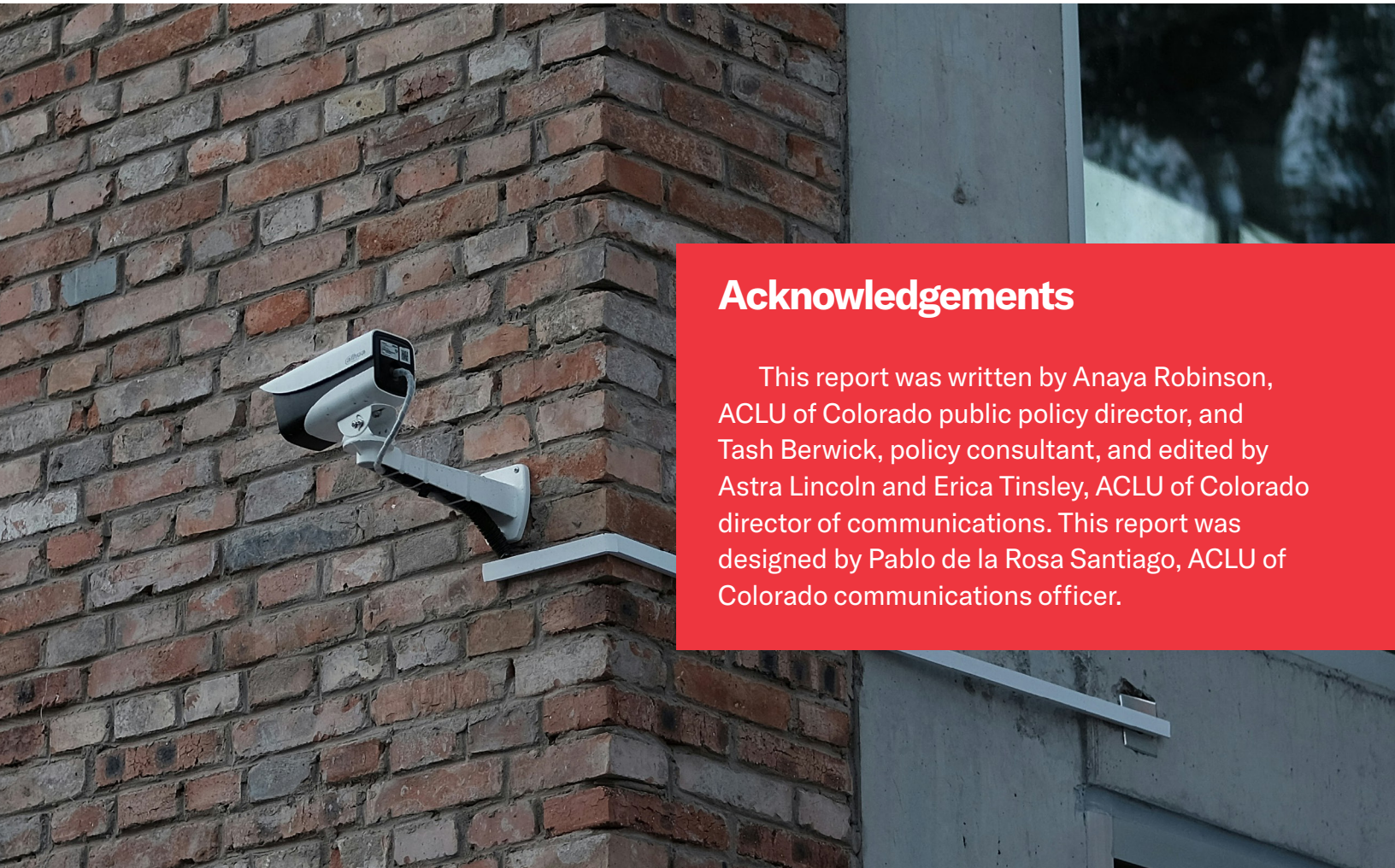
Colorado's recent privacy laws and proposed legislation reflect genuine progress in responding to the challenges of a data-driven society. However, absent a private right of action, clear definitions, and constitutional guardrails, the laws risk being underenforced or invalidated. Future legislative efforts must prioritize enforceability, rights-based design, and national coordination. To that end, Colorado policymakers should consider:

- Enacting a **private right of action** for biometric and consumer data violations;
- Adopting the National Institute of Standards and Technology's AI risk framework, or creating a more protective version, to **clarify compliance for high-risk AI deployments;**
- **Imposing clearer limits on interagency and federal data sharing,** particularly for facial recognition systems;
- **Creating narrowly tailored social media regulations** that do not rely on age verification systems that pose significant privacy and constitutional concerns;
- **Expanding transparency and disclosure obligations** across all regulated sectors;
- **Amending SB24-205 to increase protections and enforcement** for consumers, clarifying definitions, and maintaining the effective date;
- **Including the public sector in the CPA** and minimizing exemptions; and
- **Regulating government use of all AI,** not just facial recognition services.

By grounding privacy laws in constitutional principles, procedural fairness, and technical feasibility, **Colorado can serve as a national model for responsible tech regulation.** ☐

References

- Brown v. Entm't Merchs. Ass'n, 564 U.S. 786 (2011).
- Carpenter v. United States, 138 S. Ct. 2206 (2018).
- Colo. Rev. Stat. § 6-1-1301 et seq. (2023).
- Doe v. Reed, 561 U.S. 186 (2010).
- NetChoice v. Griffin, No. 4:23-cv-00772 (E.D. Ark. 2023).
- NetChoice v. Bonta, No. 5:22-cv-08861 (N.D. Cal. 2024).
- Reno v. ACLU, 521 U.S. 844 (1997).
- Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d1197 (Ill. 2019).
- SB22-113, 73rd Gen. Assemb., 2d Reg. Sess. (Colo. 2022).
- SB24-205, 74th Gen. Assemb., 2d Reg. Sess. (Colo. 2024).
- Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).
- Spokeo, Inc. V. Robbins, 57 U.S. 330 (2016).
- United States v. Playboy Ent. Grp., 529 U.S. 803 (2000).
- White House Office of Science and Technology Policy. (2022) Blueprint for an AI Bill of Rights.
- American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).



Acknowledgements

This report was written by Anaya Robinson, ACLU of Colorado public policy director, and Tash Berwick, policy consultant, and edited by Astra Lincoln and Erica Tinsley, ACLU of Colorado director of communications. This report was designed by Pablo de la Rosa Santiago, ACLU of Colorado communications officer.

ACLU
Colorado

Denver, CO
aclu-co.org
@acluofcolorado