

Analyzing Colorado's New ADMT Law (SB 189)

David M. Stauss, FIP, CIPP/US, CIPP/E, IAPP Emeritus Fellow
Stauss PLLC
david.stauss@staussfirm.com

Roadmap

01

Background

02

SB 189 Explained: The New Framework

03

California v. Colorado

04

Developer Obligations

05

Deployer Obligations

06

Exemptions

07

Enforcement

08

Liability

Background

The Colorado AI Act: A First-in-the-Nation Law

The Colorado AI Act (SB 205) became law in May 2024. It was the **first state-level AI law** to create obligations for developers and deployers of **high-risk AI systems**.

The law was originally set to go into effect on **February 1, 2026**, giving developers and businesses nearly two years to prepare for compliance.

Fast Facts: SB 205

- Signed into law: **May 2024**
- Original effective date: **February 1, 2026**
- Extended effective date: **June 30, 2026**
- Scope: High-risk AI systems
- Focus: Algorithmic discrimination
- Enforcer: Colorado Attorney General

What the Original Law Required

The Colorado AI Act imposed broad obligations on both AI **developers** and **deployers** of high-risk AI systems — defined as AI systems that make or are a substantial factor in making consequential decisions.

Consequential Decisions

Decisions affecting financial services, health care, housing, and employment — among other high-stakes areas

Duty of Care

Developers and deployers were subject to a duty to use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination

Risk Management

Law contained provisions for risk management programs, impact assessments, and annual reviews

Disclosures

Developers required to make certain information available to deployers about how systems were trained and operated; Deployers had to provide notices and rights to consumers

Timeline

- 1 — May 2024**
Colorado AI Act (SB 205) signed into law. Original effective date: February 1, 2026.
- 2 — 2025 Regular Session**
Legislature considered bills to amend the law. Negotiations broke down. No agreement reached.
- 3 — August 2025**
Special legislative session called. Legislature agreed only to extend effective date to June 30, 2026.
- 4 — October 2025**
Governor Polis appointed work group to draft recommendations for revising the law.
- 5 — March 2026**
Polis announced the workgroup agreed on a policy framework to replace the Colorado AI Act.
- 6 — May 2026**
SB 189 introduced, passed both chambers, and signed into law.

SB 189 Explained: The New Framework

The Big Picture: A Paradigm Shift

SB 189 is **significantly more business-friendly** than the law it replaces. It removes many hallmarks of the Colorado AI Act in favor of a **disclosure-based framework** with limited rights in narrow circumstances.

1 ❌ SB 205 (Old Law)

- High-risk AI system framework
- Algorithmic discrimination protections
- Duty of care obligations and rebuttable presumption
- Risk management programs
- Impact assessments
- Annual reviews
- Attorney general notices
- AI interaction disclosures

2 ✅ SB 189 (New Law)

- ADMT framework
- Disclosure-based approach
- Developer documentation obligations
- Deployer notice requirements, post-adverse outcome disclosure, limited consumer rights upon adverse decisions, record retention
- No duty of care, no impact assessments

Key Takeaways: SB 189 at a Glance

New Terminology

"High-risk AI systems" replaced by "automated decision-making technology (ADMT)"

Disclosure Focus

For deployers, SB 189 centers on: pre-use consumer notices, 30-day post-adverse outcome disclosures, three-year recordkeeping, and limited consumer data access and human review rights

AG Enforcement Only

Only the Attorney General can enforce SB 189, via the Colorado Consumer Protection Act. No private right of action. A 60-day right to cure sunsets January 1, 2030.

Jan. 1, 2027 Deadline

SB 189 takes effect January 1, 2027 — ending years of uncertainty about whether a Colorado AI law would go into effect.

Complex Nuances

The bill is complex, with many intertwined definitions and numerous exceptions. Businesses must explore each exception and qualification carefully in the context of their specific operations.

Automated Decision-Making Technology

Statutory Definition: ADMT means a technology that **processes personal data** and uses computation to generate output, including predictions, recommendations, classifications, rankings, scores, or other information that is used to **make, guide, or assist a decision, judgment, or determination** concerning an individual.

Excludes

- Anti-malware
- Anti-virus
- Calculators
- Databases
- Data Storage
- Firewalls
- Internet domain registration
- Internet website loading
- Networking
- Spam- and robocall-filtering
- Spell-checking
- Spreadsheets that require human analysis and do not use machine learning, foundation models, or LLMs
- Web caching
- Web hosting

ADMT: Key Exclusions

Human Review / Administrative Processing

The definition excludes tools used by individuals solely to summarize, organize, translate, draft, route, or present information for human review or administrative processing.

Chat Feature Exemption

ADMT excludes technology that communicates with consumers in natural language or other means readily understood by an average consumer for the purpose of providing consumers with information, making referrals or recommendations, answering questions, or generating other content — IF:

- The technology is not contracted, advertised, marketed, configured, or intended by a person to be used in a consequential decision, AND
- The technology is subject to an acceptable use policy that prohibits generated content from being used in a consequential decision.

The "Materially Influence" Standard

 **Statutory Definition:** "Materially influence" means an ADMT output is a **non-de minimis factor** that is used in making a consequential decision and an ADMT output that affects the outcome of a consequential decision, including by **constraining, ranking, scoring, recommending, classifying**, or otherwise meaningfully altering how a consequential decision is made.

Attorney General Rulemaking

Attorney General is given permissive rulemaking authority to clarify standard.

The definition explicitly **excludes** incidental, trivial, or clerical uses of ADMT output.

What Is a "Consequential Decision"?

 A decision, determination, or action made about a **consumer** that relates to the **provision of** or a consumer's **access to, eligibility for, selection for, or compensation for a covered domain** — or a decision, determination, or action about a consumer that relates to a **differentiated price, cost sharing, compensation, or other material terms** in a manner that is reasonably likely to materially limit, delay, effectively deny, or otherwise fundamentally alter the consumer's access, eligibility, or opportunity for a **covered domain**.

Nine Exemptions

Low-stakes or routine uses

Advertising and content tools

Basic spreadsheets

Tools that just summarize or organize information

Narrow procedural or data-processing tasks

Security activities (cybersecurity, spam filtering, anti-money laundering controls)

Activities relating to technology used for the Bank Secrecy Act, USA Patriot Act, FTC Red Flags Rule, and certain sanctions programs

Fraud prevention

Routine academic administration and student support processes that do not materially influence consequential decisions

Covered Domains



Employment

Employment or an employment opportunity that creates or may create an employer-employee relationship



Education

An education enrollment or education opportunity



Housing

The lease or purchase of residential real estate in Colorado



Financial Services

A financial or lending service



Insurance

Insurance



Health Care

Health-care services



Essential Government Services

Essential government services or benefits

Who Is a "Consumer"?

The Base Definition

SB 189 starts by incorporating the Colorado Privacy Act's definition (C.R.S. § 6-1-1303(6)(a)): a "Colorado resident acting *only* in an individual or household context."

But SB 189 Expands This To Include:

- Employees (defined by reference to C.R.S. § 8-4-101(5) as "any person, including a migratory laborer, performing labor or services for the benefit of an employer")
- Job applicants who are Colorado residents
- Any individual whose access to, eligibility for, or opportunity in Colorado is evaluated in a consequential decision by a person doing business in Colorado

Practical Takeaway

The ultimate intent is to cover two groups:

1. Individuals physically present in Colorado
2. Individuals outside Colorado who are interacting with persons doing business in Colorado

This means the law's reach extends beyond Colorado residents to anyone whose opportunities in Colorado are being evaluated.

Who Does SB 189 Apply To?

Developers

A person doing business in Colorado that:

- Develops, offers, sells, leases, licenses, or otherwise makes commercially available a covered ADMT
- Develops a component that is a substantial part of a covered ADMT
- Substantially modifies an ADMT

SB 189 excludes persons that develop and use an ADMT solely for **internal research purposes** where the ADMT is not used in consequential decisions.

Deployers

A person doing business in Colorado that **deploys a covered ADMT**.

The law contains **numerous exceptions and qualifications** that businesses will need to explore carefully in the context of their specific operations.

Developer Obligations

Developer Obligations

Developers must provide deployers with the following information about each covered ADMT:

1

Intended & Harmful Uses

A general statement describing the **intended uses** and **known harmful or inappropriate uses** of the covered ADMT

2

Training Data

A description of the **categories of data**, including personal data (as defined in the Colorado Privacy Act), used to train the covered ADMT — **to the extent known**

3

Known Limitations

Known limitations of the covered ADMT, including known risks and circumstances in which the covered ADMT should **not be used**

4

Use & Review Instructions

Instructions for the deployer's **appropriate use, monitoring, and meaningful human review**, where applicable

Developer Obligations

How Documentation Can Be Provided

Developers can provide this information through **public release notes**, as long as they provide direct notice of those release notes to each deployer of the covered ADMT. Developers must also **update the information for material changes** — notifying deployers of material updates, intentional modifications, and changes to intended use or risk mitigation within a reasonable time.

Recordkeeping

Developers must retain records necessary to demonstrate compliance for **at least three years**.

Trade Secret Protection

Developers **do not need to produce trade secret information** when making these disclosures — an important protection for proprietary AI technology.

Deployer Obligations

Deployers Obligations

Deployers have **significantly more obligations than developers**, although far fewer than under the Colorado AI Act. In general, SB 189 requires deployers to:



Keep Records

Maintain records necessary to show compliance for at least three years



Provide Notice

Deliver a pre-use consumer notice and a post-adverse outcome disclosure



Honor Consumer Rights

Grant consumers experiencing an adverse outcome limited rights to access, correct data, and obtain human review

Deployer Recordkeeping

Three-Year Retention Requirement

SB 189 creates a **three-year record retention requirement** for deployers to keep records necessary to show compliance with its provisions.

The three-year period **runs from the date of the consequential decision** — meaning records must be maintained on a rolling basis for each individual decision made using covered ADMT.

What Records to Keep? Deployers must retain records **necessary to demonstrate compliance** — which will include documentation of pre-use notices provided, post-adverse outcome disclosures sent, consumer rights requests received, and how each was handled.

Consumer Disclosure: Two Requirements

SB 189 creates **two distinct consumer disclosure obligations** for deployers: a pre-use notice and a post-adverse outcome disclosure.

1. Pre-Use Notice

Required **prior to** deployers using a covered ADMT to materially influence a consequential decision

Must be **clear and conspicuous** — a deployer can comply by maintaining a "prominent public notice that is reasonably accessible at points of consumer interaction, including through a link or posting that is reasonably proximate to the interaction or transaction"

Must provide instructions for how consumers can obtain additional information required by SB 189

2. Post-Adverse Outcome Disclosure

Required when a covered ADMT materially influences a consequential decision that results in an **adverse outcome** for a consumer

Must be provided **within 30 days** of the adverse decision

Must include a **plain-language description** of the consequential decision, the ADMT's role, instructions for requesting additional information, and an explanation of consumer rights

The 30-Day Post-Adverse Outcome Disclosure

When Is It Triggered?

Triggered when a deployer uses a covered ADMT to **materially influence a consequential decision** that results in an **adverse outcome** for a consumer.

What Is an 'Adverse Outcome'?

- ❏ A decision that denies, terminates, revokes, or materially reduces or restricts a consumer's access to, eligibility for, selection for, compensation for, or the provision of an opportunity or service
- A decision that results in materially less favorable differentiated price, cost, compensation, or other material terms that are reasonably likely to materially limit, delay, effectively deny, or otherwise fundamentally alter access compared to similarly situated consumers

If a decision outcome imposes materially less favorable differentiated pricing or terms, it materially influences price, cost sharing, compensation, or material terms.

What Must the Disclosure Include?

- A **plain-language description** of the consequential decision
- A description of the **ADMT's role** in the decision
- Instructions for **requesting additional information**
- An explanation of **consumer rights** (including correction and human review rights)

- ❏ The Attorney General must adopt rules to clarify post-adverse outcome disclosure requirements by **January 1, 2027**.

Exceptions & Special Rules

ECOA & FCRA Coordination

Businesses already providing post-adverse notices to comply with the Equal Credit Opportunity Act (ECOA) or Fair Credit Reporting Act (FCRA) are not required to provide duplicative notices — so long as the existing notice covers the information required by SB 189.

Federal Law & Security Exceptions

Businesses are not required to provide post-adverse outcome notices if doing so would:

- Be prohibited by federal law, OR
- Compromise the confidentiality or integrity of cybersecurity, fraud prevention, anti-money laundering, counter-terrorist financing, or economic sanctions compliance programs required by law.

FERPA-Regulated Entities

SB 189 provides specific rules for entities regulated under the Family Educational Rights and Privacy Act (FERPA) regarding how to provide post-adverse outcome notices.

Consumer Rights Under SB 189

When a consumer receives an adverse outcome from a covered ADMT, SB 189 grants them **limited rights**. These rights are only triggered upon an adverse consequential decision — they are not general ongoing rights. Rights are tied to Colorado Privacy Act (CPA), triggering CPA exceptions.

1

Right to Access Personal Data

Consumers can **request the personal data** that was used by the covered ADMT in making the consequential decision

2

Right to Correct Data

Consumers can request **correction of factually incorrect personal data** used by the covered ADMT

3

Right to Meaningful Human Review

Consumers have the right to request **meaningful human review and reconsideration** following a covered ADMT making a consequential decision that results in an adverse outcome

Human review rights apply **"to the extent commercially reasonable"** — providing deployers some flexibility in implementation.

The Right to Correct: Scope & Limitations

-  SB 189 carves out certain exceptions from the Colorado Privacy Act (CPA) — but only for the right to correct factually incorrect or materially inaccurate personal data. These carveouts do NOT apply to the right to access. This creates a practical tension: consumers may have difficulty correcting data they have no right to access.

CPA Exceptions That Do NOT Apply to the Right to Correct

1. Employment data
2. Public utility or authority data
3. State institution of higher education data
4. State and county/city/municipality data for noncommercial purposes

What Cannot Be Corrected

The right to correct does not require correction of:

- Opinions
- Predictions
- Scores
- Protected evaluations

What Is "Meaningful Human Review"?

The Statutory Standard

SB 189 defines "meaningful human review" as a process by a **trained individual with authority to approve, modify, or override the decision**, who:

- **Doesn't defer** to the system's output
- Can review the system's **purpose, limits, and data used**

The "Commercially Reasonable" Qualifier

Human review is required only **"to the extent commercially reasonable"**, so deployers may defend the lack of review if it's not feasible in context.

Exemptions

Insurers

Exemption

Insurers subject to C.R.S. § 10-3-1104.9 are exempt from SB 189.

If Not Complying with That Law

Insurers not complying with C.R.S. § 10-3-1104.9 must still provide notice of use of covered ADMT.

Employer Carve-Out

Insurers still must comply with SB 189 in their role as employers. The exemption does not extend to employment-related use of covered ADMT.

HIPAA Covered Entities

Broad Exemption (with Exception)

All provisions of SB 189 — except the liability provision — do not apply to HIPAA covered entities.

General Notice Requirement

Must provide patients with general notice of use of advanced technologies, including covered ADMT. This can be incorporated into other existing notices.

Financial Assistance Disclosure

If using covered ADMT to determine a patient's eligibility for financial assistance, must provide a disclosure and information on how to request meaningful human review where applicable. This can be provided through an adverse outcome notice.

PHI Protection

SB 189 does not require disclosure of protected health information (PHI).



Employer Carve-Out

HIPAA covered entities still must comply with SB 189 in their role as employers.

Medical Devices & GLBA Data

Medical Devices

All provisions of SB 189 — except the liability provision — do not apply to medical devices subject to US FDA regulation.

GLBA Data

SB 189 does not require any person to disclose nonpublic personal information (NPI) in violation of the Gramm-Leach-Bliley Act (GLBA).

Enforcement

Enforcement

Attorney General as Sole Enforcer

The Colorado **Attorney General** is charged with enforcing SB 189 under the **Colorado Consumer Protection Act**. A violation of the bill constitutes a **deceptive trade practice** under that statute.

The Attorney General is the **exclusive public enforcer**. SB 189 **does not create a private right of action**, so consumers may not sue developers or deployers directly under the law.

Key Enforcement Features

- Enforced through the **Colorado Consumer Protection Act**
- Violations treated as **deceptive trade practices**
- **Attorney General** is the sole public enforcer
- **No private right of action**
- 60-day **right to cure** before AG action, subject to exceptions and sunset

The Right to Cure — and Its Sunset

How the Right to Cure Works

Before the Attorney General may initiate an enforcement action, it must provide the developer or deployer with a **60-day notice and opportunity to cure** the alleged violation — if a cure is deemed possible.

The AG does not have to offer a cure period for **knowing or repeated violations**.

The Sunset: January 1, 2030

Senate Majority Leader Rodriguez insisted on **sunsetting the right to cure** — the most notable change from the workgroup bill. The right to cure expires on **January 1, 2030**.

Liability

Developer-Deployer Liability Allocation

Fault Allocation Rules

The bill clarifies how fault should be allocated between developers and deployers in **civil actions alleging unlawful discrimination** under existing law — not under SB 189 itself (which has no private right of action).

This provision recognizes that the developer and deployer may have different levels of knowledge and control over the ADMT's behavior in any given use case.

Void Contract Clauses

Any **contract clause that attempts to shift ADMT discrimination liability** between a developer and deployer is **automatically void** under SB 189.

This means businesses cannot contractually disclaim or shift liability for ADMT-related discrimination — a provision with significant implications for AI vendor contracts and terms of service.