iapp x DG

Does your AI count:

Scoping ADMT before California's January 1, 2027 deadline

Monday, 14 September
08:00-09:00 PDT
11:00-12:00 EDT
17:00-18:00 CEST

David Khalily
Senior Privacy & AI Counsel
Harvey

Omer Tene
Partner
Goodwin

Neelofer Shaikh
Attorney
CalPrivacy

Daniel Barber
Co-founder & CEO
DataGrail

HOW THE HOUR RUNS

From the rules to your roadmap

1. **ADMT, explained.** What the CCPA rules actually require, with CalPrivacy.
2. **Why it matters now.** The Jan. 1, 2027 deadline, enforcement, and recent litigation
3. **What counts.** Defining a "significant decision" and the human-in-the-loop test.
4. **Where it shows up.** The back-office and everyday tools that qualify.
5. **What to do about it.** Building a defensible inventory and risk assessment.

CalPrivacy Overview of ADMT Regulations

The full text of these regulations can be found in Articles 10 and 11 of the California Code of Regulations, title 11, Division 6, Chapter 1, available at cppa.ca.gov/regulations.
Please be aware that this overview presentation is not an exhaustive list or substitution for ensuring compliance with all applicable statutory and regulatory requirements.

What is “automated decisionmaking technology” (ADMT)?

- Technology that processes **personal information**
- Uses **computation**
- Replaces or **substantially replaces human decisionmaking**

  This means the business uses the technology’s output to make a decision ***without human involvement***

ADMT includes profiling that replaces or substantially replaces human decisionmaking.

Reference: 11 CCR § 7001(e)

What does “human involvement” require a human reviewer to do?

Know how to interpret and use the output to make the decision	+	Review and analyze the output, and any other information relevant to make or change the decision	+	Have the authority to make or change the decision based on that analysis

Reference: 11 CCR § 7001(e)

Which decisions are in scope?

Significant Decisions

A significant decision is a decision that results in the provision or denial of:

- Financial or lending services
- Housing
- Education enrollment opportunities
- Employment or independent contracting opportunities or compensation
- Healthcare services

Reference: 11 CCR § 7001(ddd)

What must a business do before using ADMT for a significant decision?

Risk Assessment → Pre-use Notice → Opt-out of ADMT → Access ADMT

NOW	NO LATER THAN JANUARY 1, 2027
Risk Assessment	Pre-use Notice; Opt-out of ADMT; Access ADMT

Reference: Articles 10 and 11

For more information, please visit:

https://cppa.ca.gov/regulations/

THE CLOCK

Two dates, one narrowing window

Jan. 1, 2026

CCPA general regulations take effect
Includes obligation to conduct risk assessments for new use of ADMT to make significant decisions

we're here

Jan. 1, 2027

Specific compliance deadline for CCPA-required pre-use notices, opt-outs, disclosures and access rights

The takeaway: The general rules are already live and require risk assessments for net-new significant decision-making via ADMT, as well as a look-back exercise for in-scope activities that began before 2026. The 2027 deadline adds an additional layer - pre-use notices, opt-out compliance, and additional disclosures and consumer access rights.

WHAT TRIGGERS ADMT

Five decisions the rule cares about

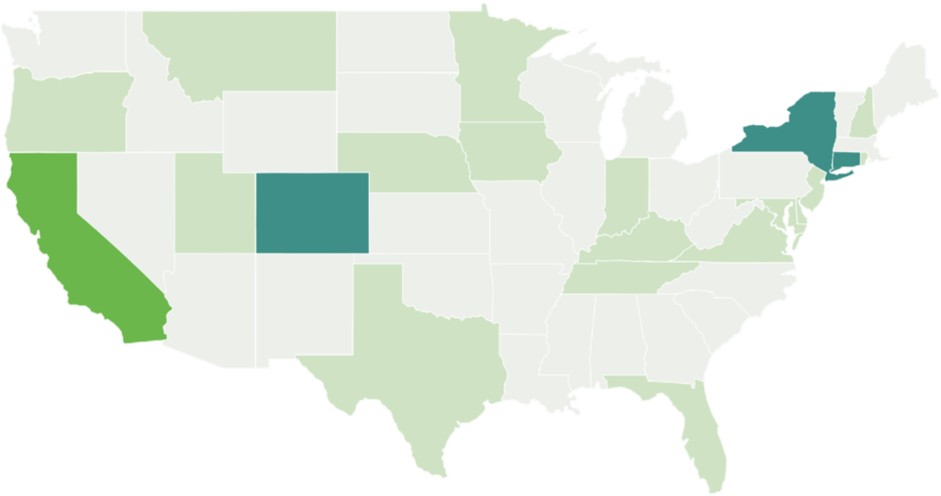
ADMT obligations attach when automated technology drives a "significant decision" about a consumer in...

- Employment
- Lending
- Housing
- Healthcare
- Education

The point: These aren't customer-facing chatbots. They're the back-office systems that decide who gets hired, funded, housed, treated, or admitted.

THE BIGGER PICTURE

California is first, not alone



California

ADMT, the most detailed automated-decision rules

CO · CT

Profiling opt-out rights already in force

NYC Local Law 144

AEDT, bias audits for automated employment decision tools

17 more states

Comprehensive privacy frameworks in effect today (24 total state laws enacted through 2026)

ENFORCEMENT RISK

CCPA enforcement is already real

Recent California settlements — broader CCPA obligations, not ADMT yet:

HONDA	GM	Walt Disney
$630K+	$12.75M	$2.75M

Reframe for the room: Enforcement is happening today under existing rules. ADMT adds a new significant-decision layer on top of it.

LITIGATION RISK

AI decision tools already in active litigation

AI decision tools already in active litigation across employment and housing:

Mobley v. Workday, Inc.

The Allegation: Job applicants alleged that a vendor's algorithmic screening platform systematically excluded candidates based on protected characteristics like race, age, and disability.

Kistler v. Eightfold AI Inc.

The Allegation: Plaintiffs challenged a predictive recruiting engine that ingests vast consumer datasets to generate opaque, numerical candidate suitability scores.

Former Employees v. Meta Platforms, Inc.

The Allegation: An internal workforce analytics system autonomously monitored employee digital activity and telemetry data to execute algorithmic terminations.

DEFINING THE LINE

"Significant decision" = substantially replaces human judgment

If the technology makes, or substantially drives, a decision that meaningfully affects a person, and no human is genuinely in the loop, it's in scope.

WORKED EXAMPLE

- A model scores job applicants and the recruiter only ever sees the top 5% it surfaces. ***In scope — the tool has effectively made the cut.***
- A model flags applications, but a recruiter reviews the full pool and can pull anyone forward. ***Likely assistive — a human still decides.***

THE FIRST FORK

“A human could override it.” Real test or hopeful argument?

Out of scope

GENUINELY ASSISTIVE

- A human reviews the real inputs, not just the output
- Override happens in practice, not just on paper
- The person can reach a different result and does

In scope

AUTOMATED IN EFFECT

- The human rubber-stamps what the system surfaces
- Override is theoretically possible but never used
- The tool's output is the decision, minus a signature

1

The systems nobody's auditing

- Which back-office tools sit closest to ADMT exposure?
- Does each person rank the risk the same way?

Customer-facing AI gets the scrutiny. These don't.

HR tech

Screening, ranking, and attrition scoring that shapes who advances.

Fraud scoring

Models that decline, freeze, or flag customers with little human review.

Underwriting

Lending and pricing engines making the call before anyone looks.

The gap: They get far less scrutiny than customer-facing AI, and they're just as likely to qualify as ADMT.

2

The inventory-triage framework

- What's the fastest realistic path to a defensible inventory?
- What does a genuine risk assessment look like versus a checkbox?

Inventory, then classify, then prioritize

1

Inventory

Surface every automated system — including the ones nobody registered.

→

2

Classify

Test each against the significant decision line: in scope, assistive, or unclear.

→

3

Prioritize

Rank by decision type and volume — highest-stakes, highest-throughput first.

Honest goal for most teams: a documented, good-faith remediation plan by Jan. 1, 2027.

THE THROUGHLINE

What this means for your program

Assume your own AI tools are in scope too. Review them when you scope, not just vendor tools.

Start with the most under-scoped systems: the back-office ones like HR, fraud, and underwriting.

Do a documented, genuine risk assessment. It's what keeps you defensible instead of exposed if you're ever asked.

HOW DATAGRAIL HELPS

From discovery to documented risk

Discover

Find AI and MCP systems across your stack — including the ones nobody registered.

Classify

Score each system for ADMT exposure against the significant-decision line.

Assess

Generate risk assessments drafted from real system context, ready to defend.

Questions and Answers

Drop your questions in the panel — we'll take as many as time allows.

David Khalily

Omer Tene

Neelofer Shaikh

Daniel Barber

Want to learn more? Let's chat!

datagrail.io

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ9fxX

Thank you in advance!

For more information: www.iapp.org

iapp

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact:

livewebconteam@iapp.org