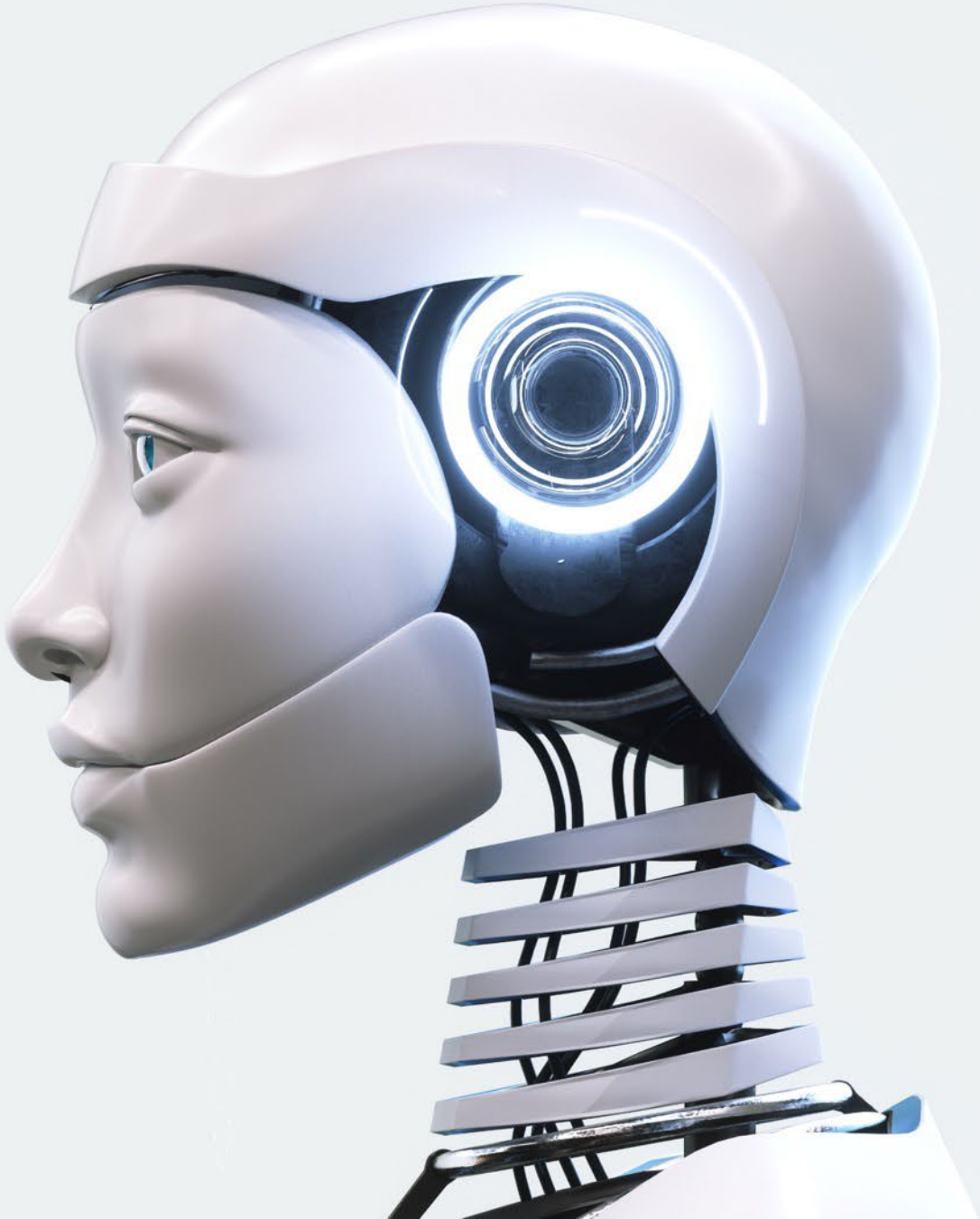
JENNER&BLOCK

CLE RELAY

AI Challenges and Opportunities in the Legal Space

Agenda

- Deciphering the White House's AI Policy
- State Legislative/Regulatory Developments
- Privilege and Work Product
- AI Governance Best Practices



Deciphering the White House's AI Policy

JENNER&BLOCK

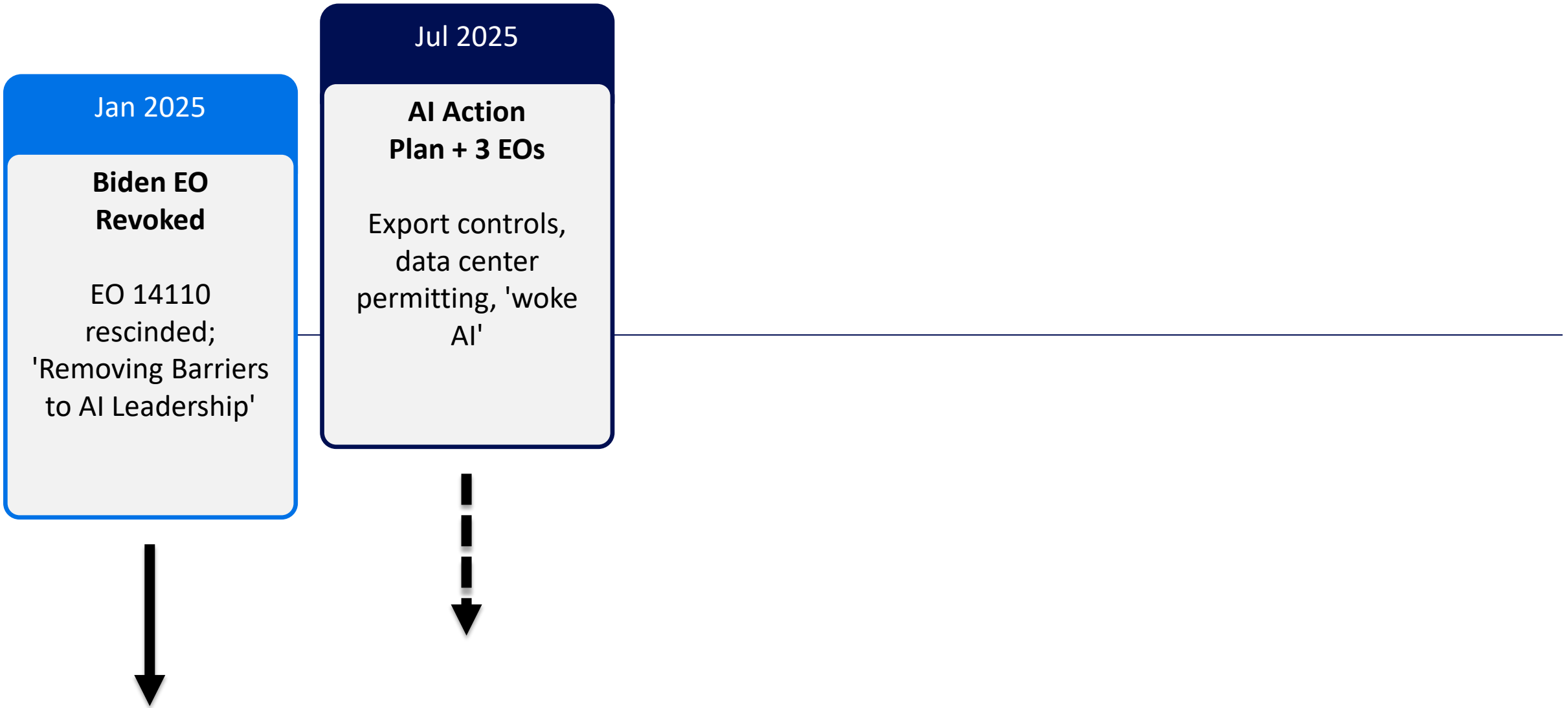
The Policy Arc

Jan 2025

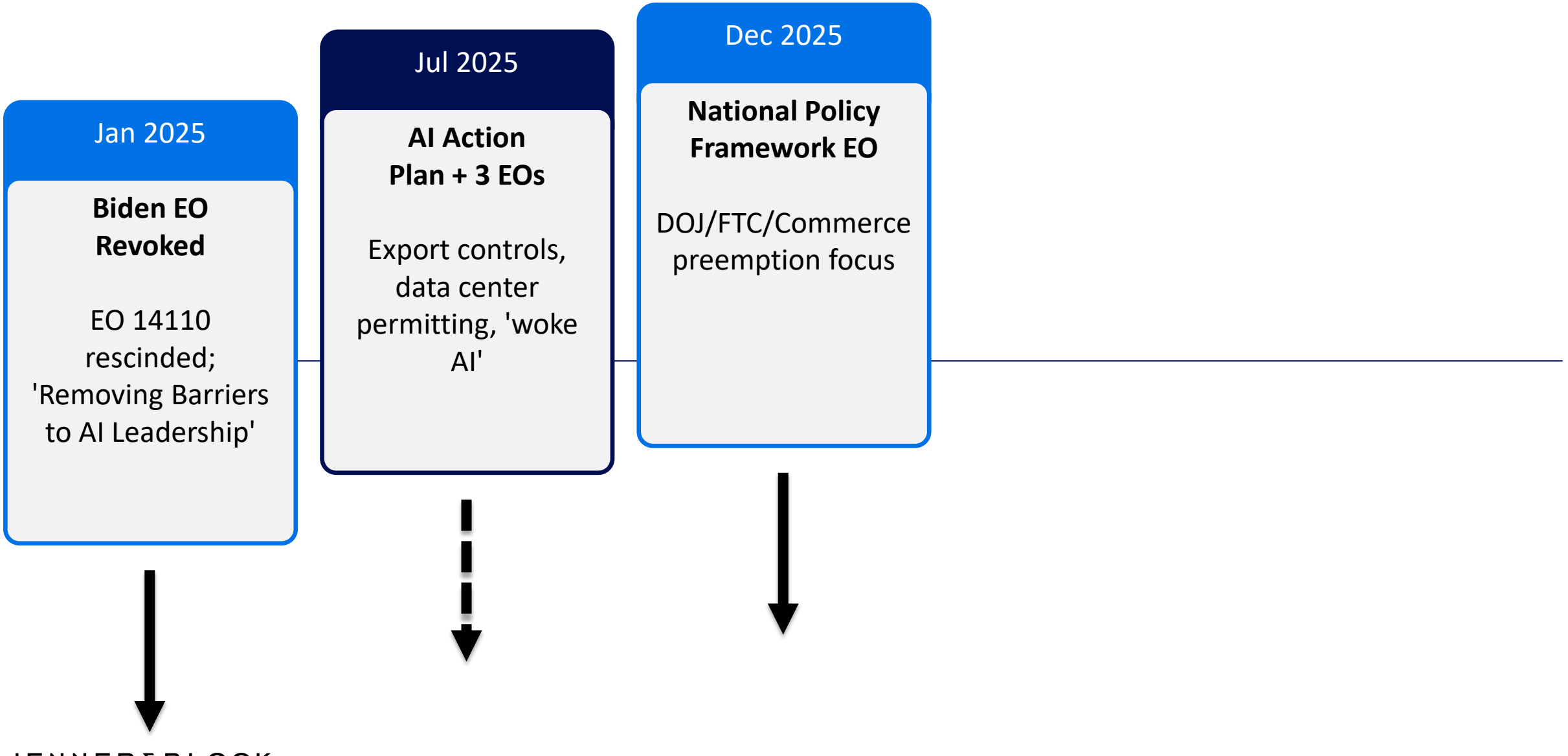
Biden EO Revoked

EO 14110 rescinded; 'Removing Barriers to AI Leadership'

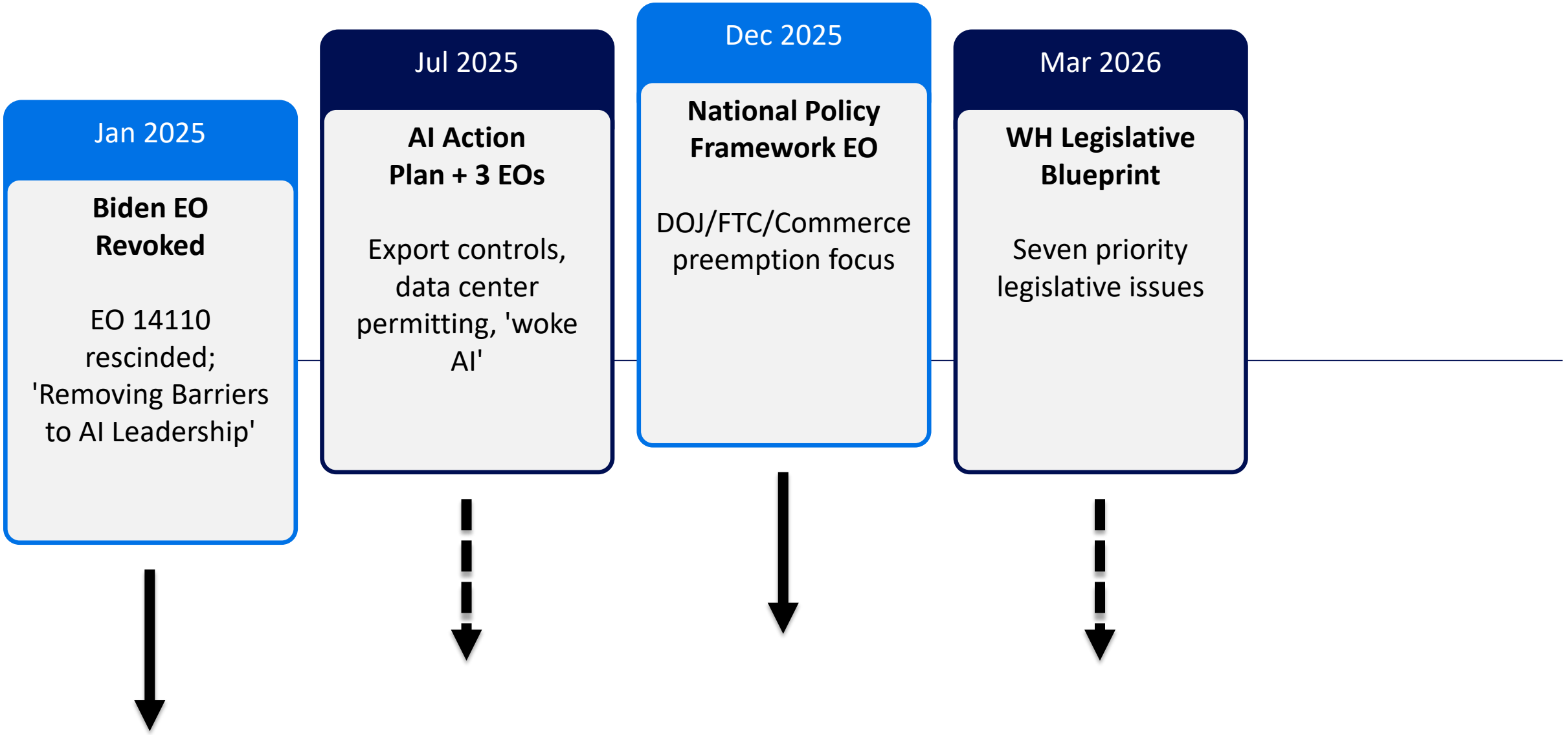
The Policy Arc



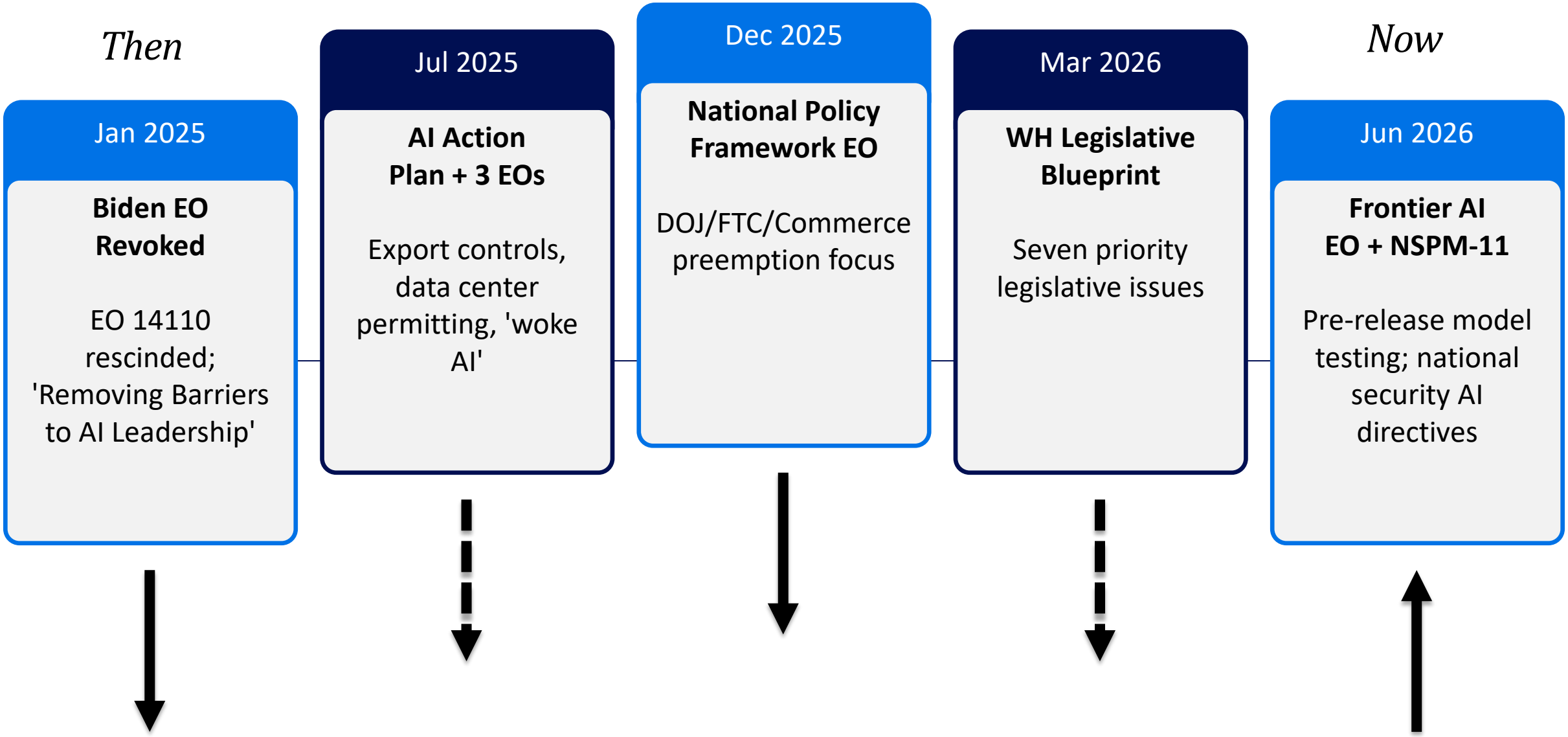
The Policy Arc



The Policy Arc



The Policy Arc



What Changed?

June 2 EO — *Promoting Advanced AI Innovation and Security*

Core Policy: Voluntary pre-release review

AI developers — on a voluntary basis — may submit frontier models to federal agencies up to 30 days before public release for testing.

Key parameters still to be set

NSA to define what constitutes a covered model, but that definition will be classified. Confidentiality and non-disclosure protections also undefined.

Government playing a new gatekeeping role

The EO enables the government to help select who receives early access to powerful models. Treasury also establishing an information-sharing clearinghouse for critical infrastructure vulnerabilities.

Not a mandatory government approval gate

Non-participation could affect government relationships and contracting, as well as public perception. At the same time, participating could trigger government action to restrict access.

June 5 — NSPM-11: *AI in the National Security Enterprise*

Four pillars: Adopt, Adapt, Assure, Account

Directs military and intelligence community to close the gap between commercially available AI and what national security professionals use, acknowledges need for assurance and accountability measures.

Contract termination power

Agencies directed to terminate, 'to the maximum extent permissible by law,' contracts with companies showing a repeated 'pattern of conduct inconsistent' with NSPM-11 policy.

Guidance Still to Come

Implementation will matter - directs departments and agencies to develop additional guidance for the use of AI in national security systems.

AI National Security Strategic Reserve

New civilian talent pool of non-government AI experts who can be called upon for national security needs — raising questions about IP and compelled participation.

Broader Themes Worth Tracking

01 Geopolitical Competition Driving White House AI Policy

02 Government Contracting as a Major AI Compliance Lever

03 Federal Government is Coordinating AI Security Information

04 Federal/State Questions Remain Live

05 EO Directives v. Agency Implementation

State Legislation and Regulation

JENNER&BLOCK

Federal AI law is stalled. The states didn't wait.

- There is no comprehensive federal AI statute. Washington has favored a light-touch, pro-innovation posture — so the real rules are being written in statehouses and AG offices.
- The result is a fast-growing patchwork that reaches far beyond "AI companies." If you deploy, generate, or even just interact with consumers using AI, you are likely already in scope.

1,000+

AI bills filed across all 50 states in the 2025 cycle

45

states introduced AI bills in 2024 alone

3

states with broad AI regimes — California, Colorado, and Connecticut (effective 2026–27)

Eight kinds of state AI law you can already trip over

Frontier model rules
Safety frameworks for the largest developers / most capable models

High-risk deployment
Duties when AI drives consequential decisions

Watermarking / provenance
Label AI-generated audio, image, video

Transparency / chatbots
Tell people when they're talking to AI

Deepfakes
Penalties for manipulated media

Digital replicas
Protect voice & likeness from cloning

Model training data
Disclose what data trained the model

AI companions
Implement safety guardrails for users, including minors

It's not just "AI companies"

Many of these laws turn on how AI is USED, not on whether you build it. Everyday business and law-firm uses can fall squarely within scope:

Customer-facing chatbots
Disclosure laws may require telling users they're talking to AI.

Hiring & HR screening
"High-risk" decision rules reach employment tools.

Marketing & generated media
Provenance / watermarking and deepfake laws attach to AI images, audio, video.

Healthcare & advice
Bans on AI posing as licensed professionals; AG consumer-protection scrutiny.

Lending & housing decisions
Consequential-decision duties and impact assessments.

Client & consumer data
Privacy and data-use rules overlap with AI features.

California: testing ground for the nation

California closed its 2025 session as **the AI-governance leader** — moving from one-off fixes to a full framework, and pairing it with an AG building a team to enforce.

SB 53 — frontier models

First state law to directly regulate frontier developers: safety frameworks, transparency reports, incident reporting, and whistleblower protections. Plus a CalCompute public cluster. Penalties up to $1M per violation.

THE CENTERPIECE

SB 942 / AB 853 — provenance

"Latent" labels on AI-generated image, audio, video; obligations extend to large online platforms and capture-device makers.

SB 243 — companion chatbots

Disclosures, reporting, and self-harm protocols — enacted after the broader AB 1064 was vetoed.

AB 489 — no fake clinicians

Bars AI chatbots from posing as licensed medical professionals.

AB 2013 — training data disclosure

Requires “high-level summary” of training data.

California is staffing up — and not done

AG Bonta is hiring to enforce

California's AG is adding an AI expert and "investigative technologists" to police the new laws — a model other states are likely to copy. Bonta has already issued advisories on AI in consumer protection, privacy, and healthcare.

Compliance window is now

2026 → 2028

Effective dates for enacted California AI laws span this window. AB 2013 (training-data disclosure) and the SB 942 provenance rules begin Jan. 1, 2026.

On the horizon? Kids AI Safety Act

- Previously planned as a ballot initiative
- Would redefine "companion chatbot" and restrict dangerous capabilities (self-harm, erotic, illegal content) for kids
- Adds independent safety audits — provisions the legislature stripped out of SB 53
- Bans the sale of children's data and adds a private right of action
- Expected 2026 bills also target employment AI (SB 7), automated decisions (AB 1018), and training-data databases (AB 412)

Colorado: rewritten before it ever took effect

On May 14, 2026, Gov. Polis signed **SB 26-189** — which **repeals and replaces** the original AI Act with a leaner, disclosure-based regime. Effective **Jan. 1, 2027**.

THE OLD ACT (SB 24-205)

Risk-based framework

- Duty of reasonable care vs. algorithmic discrimination
- Deployer risk-management programs
- Algorithmic impact assessments
- AG notice of discrimination; consumer appeal rights
- Covered legal services among consequential decisions

Never took effect — repealed

THE NEW LAW (SB 26-189)

Disclosure-based ADMT model

- Targets "automated decision-making technology" that materially influences a consequential decision
- Developers: hand deployers use, data & limitation disclosures
- Deployers: pre-use notice + post-adverse-outcome notice
- Consumer rights: limited access, correction & human review
- 3-yr records; 60-day AG cure period (sunsets 2030); no private right of action

The fight before the rewrite

Apr. 9, 2026

xAI sues

Moves to enjoin the original Act on First Amendment, Commerce Clause, vagueness, and Equal Protection grounds.

Apr. 24, 2026

DOJ intervenes

First federal intervention in a state AI-law challenge — joining on Equal Protection grounds.

Apr. 27, 2026

Enforcement paused

AG will not enforce until the amendment or xAI's PI motion resolves.

May 14, 2026

Legislature acts

SB 26-189 repeals and replaces the Act — satisfying a key standstill condition and reshaping the dispute.

Long-Held State AG Authorities

States aren't reliant solely on new legislation – long-held authorities also cover AI.

Civil Rights

Consumer Protection

Employment

Data Privacy

State AGs are already acting — in both parties

44

AGs urged tech companies to protect kids on chatbots & social media

47

AGs pressed platforms to curb AI-generated deepfake sexual imagery

42

AGs demanded 13 companies safety-test and warn on their chatbots

From letters to lawsuits

- CA AG Bonta issued advisories telling businesses how existing law already applies to AI
- TX AG Paxton settled a first-of-its-kind probe into deceptive AI healthcare claims
- Pennsylvania sued Character.AI over concerns about its chatbot posing as a medical professional
- A bipartisan AG AI task force launched in Nov. 2025: "Congress hasn't put basic protections in place, and we can't wait."
- Consumer protection, privacy, and healthcare are the favored hooks — and they're technology-neutral

What this means for lawyers & law firms

Your own AI use is not exempt. Courts and bar regulators are converging on one duty: verify everything.

Sanctions are landing

Courts are sanctioning lawyers for unverified, AI-"hallucinated" citations. The standard of care is being set case by case.

Verification is going mandatory

Proposed rules (e.g., CA SB 574) would require "reasonable steps" to verify AI output, correct hallucinations, and remove biased content.

Confidentiality limits

Emerging rules bar feeding confidential client information into AI tools and bar arbitrators from delegating decisions to AI.

A starting compliance checklist

Map your AI footprint

Inventory where AI touches your work and your clients' — chatbots, hiring, marketing, drafting, decisioning.

Match uses to categories

For each use, ask which of the eight law types could attach, and in which states you operate.

Track effective dates

California spans 2026–2028; Colorado's new SB 26-189 lands Jan. 1, 2027. Calendar the deadlines that hit you.

Build the paper trail

Disclosures, impact assessments, provenance labeling, and a verification protocol for AI work product.

Disclose where required

Tell consumers when they're interacting with AI; don't let tools imply licensure they lack.

Monitor & stay flexible

Litigation and rulemaking are live — keep compliance programs adjustable as the rules shift.

Three things to leave with

01

Assume a state law applies

There's no federal AI statute, but 1,000+ state bills and broad regimes in California, Colorado, and Connecticut mean most AI uses already touch a state rule.

02

"Using" AI is enough

Coverage often turns on use, not development — chatbots, hiring tools, generated media, and even your own legal work can be in scope.

03

The ground is still moving

Litigation, a federal preemption push, and active AG enforcement mean compliance must be mapped now and revisited often.

Privilege and Work Product

JENNER&BLOCK

Conventional Technologies That Typically Do Not Undermine Privilege

- **Email**
- **Word Processing**
- **Videoconferencing**
- **File Management Systems**
- **Search Engines**

Risk #1: AI Provider as "Third Party" Viewing Data

JENNER&BLOCK

Is an AI Provider a "Third Party"?

KEY DISTINCTION

Public AI Tools

- Terms of service often permit provider to use prompts/outputs to train models
- Higher risk that disclosures undermine confidentiality

Enterprise AI Tools

- Contractual protections limit provider's use of data
- More analogous to other third-party tools

CHATGPT TERMS OF USE (EXCERPT)

> Our use of content. We may use Content to provide, maintain, develop, and improve our Services, comply with applicable law, enforce our terms and policies, and keep our Services safe. If you're using ChatGPT through Apple's integrations, see this Help Center article for how we handle your Content.
>
> Opt out. If you do not want us to use your Content to train our models, you can opt out by following the instructions in this article. Please note that in some cases this may limit the ability of our Services to better address your specific use case.

United States v. Heppner (S.D.N.Y. Feb. 17, 2026)

FACTS

Federal criminal case.

- Defendant communicated with Claude to prepare an outline of possible defenses he intended to discuss with counsel.

HOLDING

Neither ACP nor WPP applied:

- AI is not a person.
- Communications were not confidential (Anthropic's terms of service allowed use of prompts to train the AI model).
- Work product protections do not apply to a defendant in a federal criminal proceeding; applied Hickman v. Taylor (Hickman focuses on protecting attorneys ("zone of privacy"), not on protecting parties).

Warner v. Gilbarco (E.D. Mich. Feb. 10, 2026) (pro se)

FACTS

- Plaintiff used ChatGPT to prepare for the litigation.
- Pro se action.

HOLDING

Work product protections applied:

- Plaintiff's prompts reflected mental impressions and should be treated as opinion work product.
- Disclosures to AI did not waive WPP, because AI programs are "tools, not persons."

Morgan v. V2X, Inc. (D. Colo. Mar. 30, 2026) (pro se)

FACTS

- Employment discrimination case.
- Pro se action.

HOLDING

- Fed. R. Civ. P. 26(b)(3) applies in civil cases and protects work product of both parties and counsel.
- Use of public-facing AI does not automatically destroy confidentiality.
- Fact that company collects data for training does not eliminate expectations of privacy or automatically waive protections.
- As a practical matter, absent legal process, highly unlikely protected information would fall into the hands of an adversary.

Key Protections for Data in Enterprise AI Agreements

FACTS

- Prohibition on using customer data to train or improve AI models
- No secondary uses of customer data
- Data retention limits and deletion obligations (*e.g.,* session data deleted after end of session or within defined window)
- Subcontractor restrictions
- Breach notification requirements
- *Ideally*: No human review of substance of prompts/inputs or outputs by AI company personnel, except where authorized by customer or required by law

Practice Tip: These principles apply not just to enterprise LLM tools (*e.g.*, ChatGPT), but also to other third-party vendors incorporating AI functionalities.

Risk #2: Users Without “Need to Know” Access

JENNER&BLOCK

Do Enterprise AI Users Without a "Need to Know" Have Access?

- Does the enterprise tool search across all materials, or just materials to which that user has access?
- If the tool only searches materials to which a user has access, are access permissions limited to users with a "need to know"? (Very broad system folder access; legal materials shared with a large group)
- Biggest risk is that an AI tool ends up giving users *more* access than they otherwise would have

Practice Tips:

(1) Take reasonable steps to preserve privilege—perfection is not required.

(2) Evaluate/test over time to understand how the tool is working in practice, and make adjustments as needed.

Risk #3: Leakage

JENNER&BLOCK

Is There a Meaningful Risk of Leakage?

- If privileged materials are being shared appropriately with people with a "need to know," what is the likelihood that privileged advice ends up passing outside of that circle through the use of AI?
  - Reproduction of outputs including privileged advice
  - Compilations including privileged documents
- Have adequate steps been taken to address other security vulnerabilities?

Practice Tip: These concerns can largely be addressed through training and document hygiene (including labeling privileged materials).

Enterprise AI Security Vulnerabilities

Vulnerability Category	Description	Business Impact
Jailbreak Attacks	Attempts to bypass safety controls and content policies	Brand damage, compliance violations, harmful content generation
Prompt Injection	Malicious instructions hidden in user inputs	Unauthorized actions, data exposure, system compromise
Data Leakage	Extracting training data or sensitive information	Privacy violations, intellectual property theft, regulatory fines
Behavioral Manipulation	Making AI act outside intended parameters	Service disruption, incorrect outputs, user harm
Policy Violations	Content that violates organizational or regulatory policies	Legal liability, reputation damage, compliance failures

Governance Best Practices

JENNER&BLOCK

Key Aspects of Successful Generative AI Policies

TOOL AND USE CASE APPROVAL

1. AI tool approval and "funneling" into enterprise tools
2. Identification and tracking of use cases
3. Procedure for approval or denial of use cases

RESPONSIBLE USE

4. Responsible use requirements
5. Prohibited uses
6. Training on general risks and use of particular tools

SAFEGUARDS & OVERSIGHT

7. Technological backstops
8. Monitoring and adaptation

Responsible Use

INACCURACIES

- "Hallucinations": AI models confidently asserting false information
- Can occur even in response to requests that should not change substance (*e.g.*, reformatting citations)

SUBSTITUTION FOR JUDGMENT

- AI does not replace professional judgment or expertise
- Outputs require human review for accuracy and completeness

BIAS

- AI models may reflect or amplify biases present in training data
- Heightened scrutiny in HR, employment, and consumer-facing decisions

SPECIFIC DEPARTMENTS

HR / Employment

- Heightened legislative/regulatory and litigation scrutiny (e.g., *Mobley v. Workday*)

Legal Team

- ABA Formal Ethics Opinion 512

Consumer Decisions

Mitigation Strategies: Training; requirements to review outputs for inaccuracy and completeness

Vendors and Contractors

- **Address stealth use of AI**
- **Ensure responsible use of AI by third parties**
- **Protect data**
- **Obtain indemnities**
- **Ensure fair pricing**

Copyrightability of AI-Generated Works

LEGAL DEVELOPMENTS

- **Copyright Office Report (Jan. 2025)**: AI-generated works without sufficient human authorship are not copyrightable; human selection and arrangement may be protectable
- ***Thaler v. Perlmutter*** **(D.C. Cir. Mar. 2025)**: Affirmed that copyright requires human authorship; purely AI-generated works not protectable
- **SCOTUS cert. denied (Mar. 2026)**

"A Recent Entrance to Paradise" — work at issue in Thaler v. Perlmutter

Mitigation Strategies: Document human creative choices in AI-assisted works

Third-Party Intellectual Property

- Risk of "memorization" of training data
- Risk of misattribution

Indemnification Provisions in AI Tools' Terms of Service

OPENAI / CHATGPT

- Prohibits "destruction, compromise, or breach of another's system or property, including malicious or abusive cyber activity or attempts to infringe on intellectual property rights of others"
- Provides for indemnification of OpenAI for any claims arising from breach of the terms

ANTHROPIC / CLAUDE

- Prohibits use of Claude to "infringe, misappropriate, or violate intellectual property or other legal rights (including the rights of publicity or privacy)"
- Provides for indemnification of Anthropic for any claims arising from breach of the terms

Mitigation Strategies: Prohibiting efforts to elicit third-party IP

CLE RELAY
FULL SCHEDULE

JENNER&BLOCK

Session 1
International Trade in a Volatile World: Accounting for Sanctions and Tariffs in Business Decisions and Contracts

Friday, June 12
12 pm CT

Session 2
Energy for the New Data Age

Monday, June 22
1:30 pm CT

Session 3
AI Challenges and Opportunities in the Legal Space

Friday, June 26
12 pm CT

Session 4
US Supreme Court Term in Review

Tuesday, June 30
3 pm CT

Thank you!

Aaron Cooper

Partner | Washington, D.C.
+1 202 637 6333 | acooper@jenner.com

Adam Unikowsky

Partner | Washington, D.C.
+1 202 639 6041 | aunikowsky@jenner.com

Caroline Cease

Partner | Washington, D.C.
+1 202 639 6056 | ccease@jenner.com

Allison Douglis

Partner | New York
+1 212 303 2505 | adouglis@jenner.com