iapp

Making AI work for privacy

How to scale privacy operations with secure AI

Tuesday, 24 March
08:00–09:00 PST
11:00–12:00 EST
17:00–18:00 CET

Speakers

Daniel Barber
Co-founder & CEO
DataGrail

Chris Carlson
Privacy Officer and
Associate General Counsel
Aledade

Shannon Yavorsky
Global Chair, Cyber,
Privacy & Data Innovation
Orrick

Agenda

The 2026 Privacy Landscape

Regulatory complexity is outpacing privacy teams.

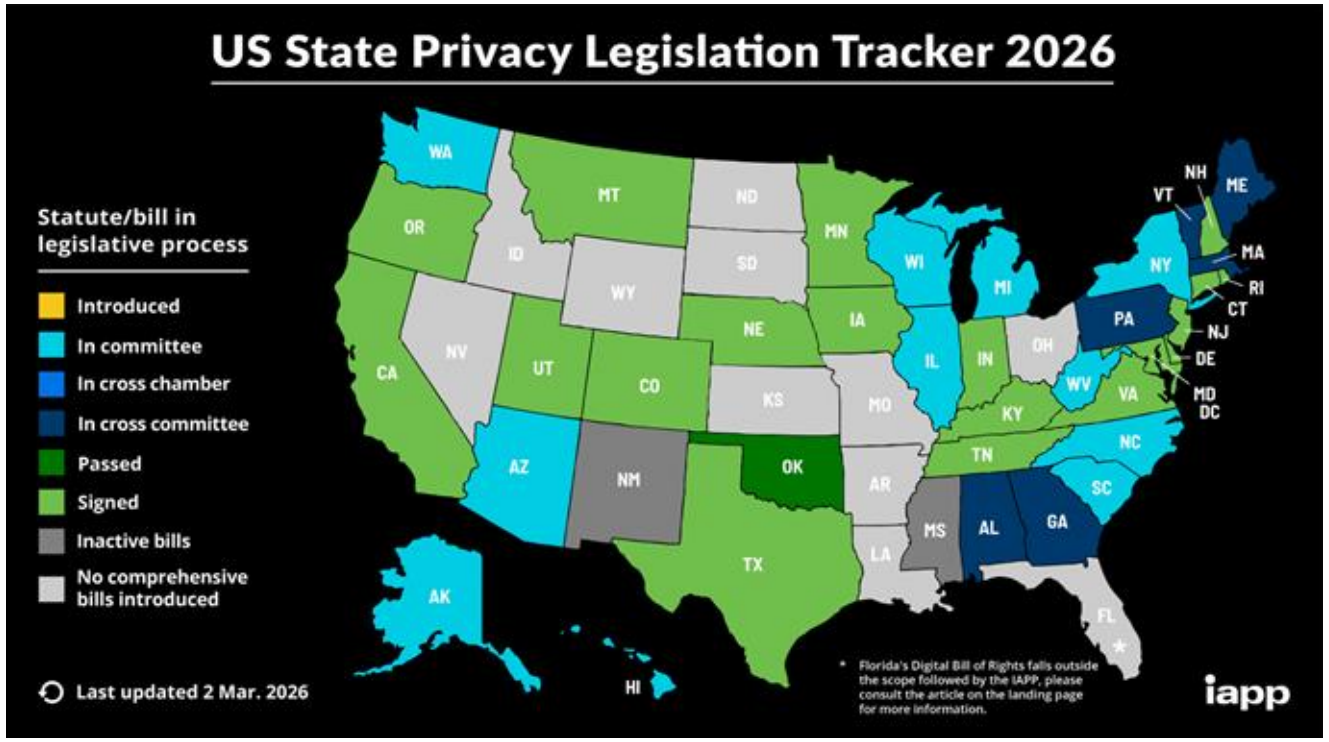
Static, manual workflows leave blind spots and gaps.

Privacy headcount can't keep up, and it's only getting worse.

Privacy work has outpaced human capacity.

It's not *if* you'll use AI, but ***how to use it responsibly.***

Privacy Risk is Growing



Source: [IAPP US State Privacy Legislation Tracker]

Ford to Change Practices, Pay Fine for Adding Unnecessary Friction to Opt-Out Process

March 5, 2026

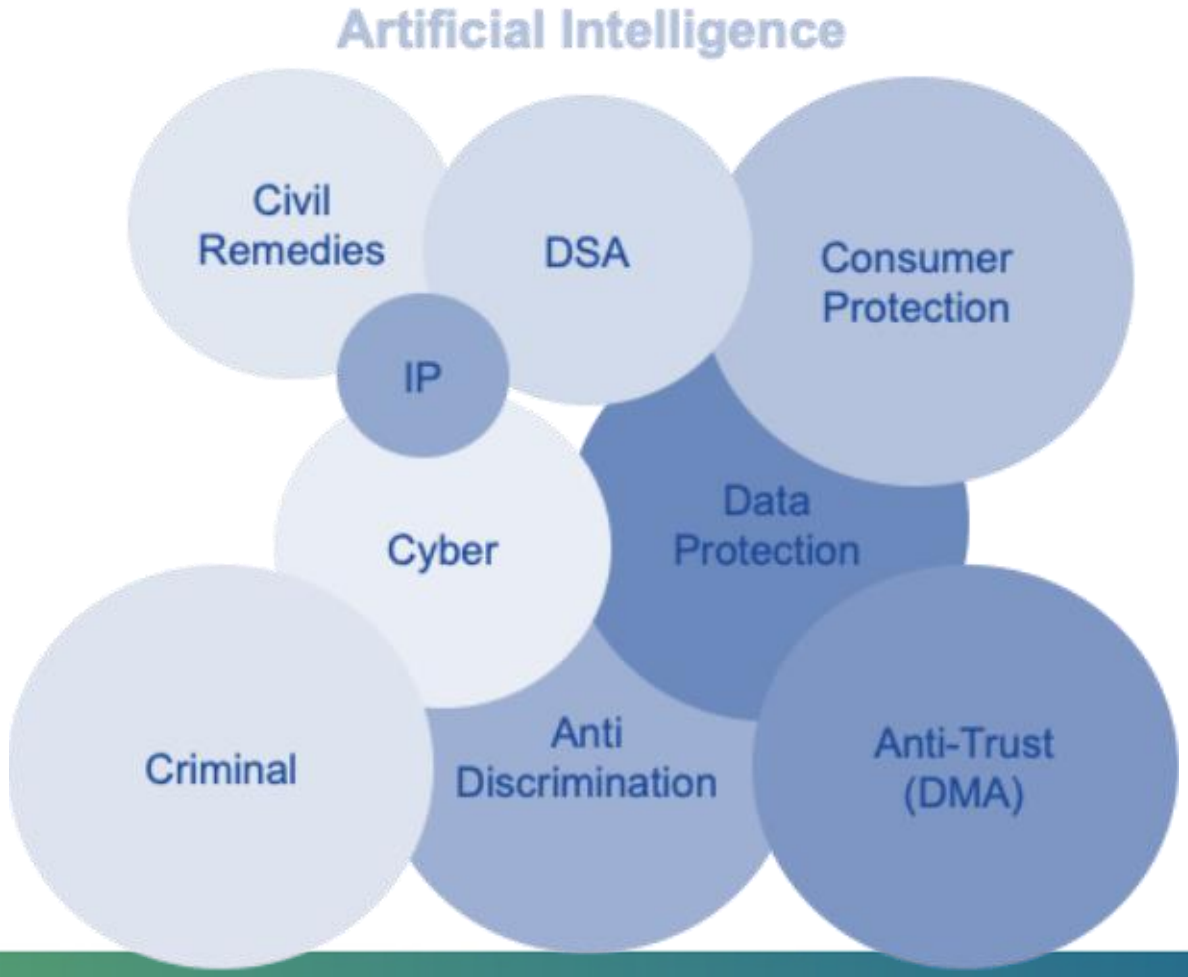
California Imposes Largest CCPA Fine to Date on Disney

February 13, 2026

Todd Snyder subjected to $345K fine over California privacy violations

The Evolving Legal Landscape

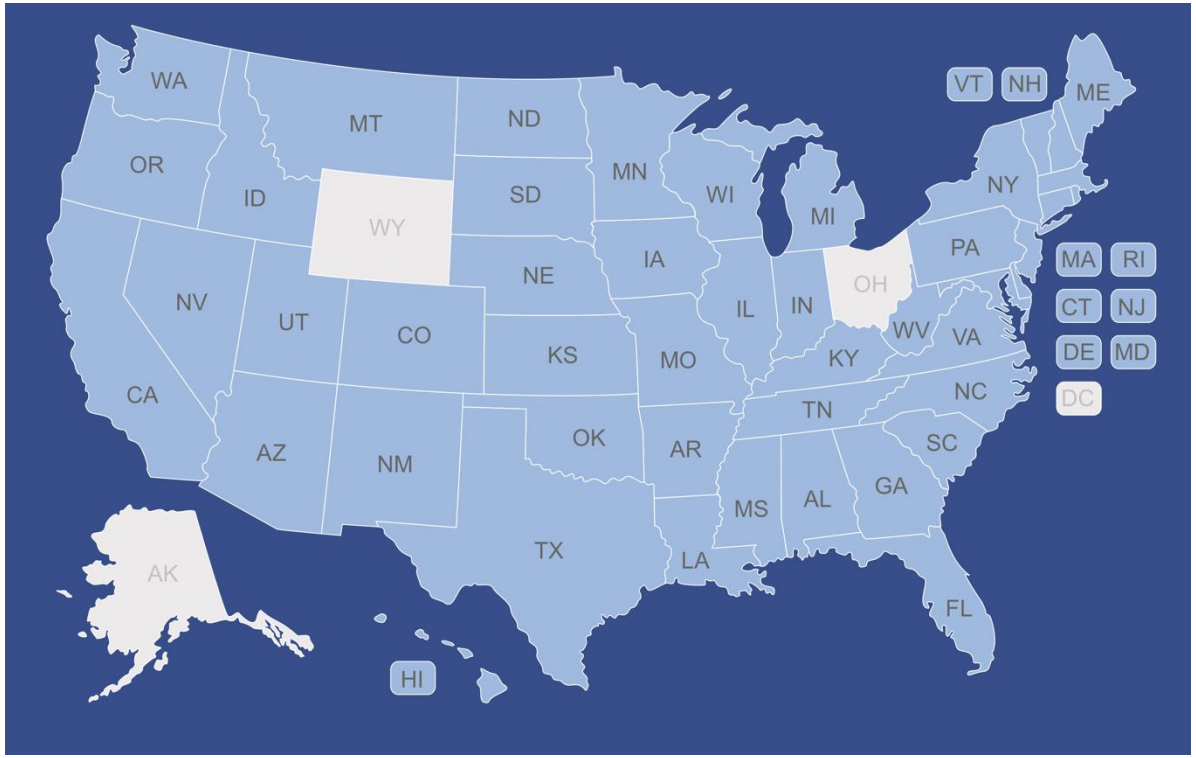
Where Does AI Fit in the Legal Landscape Today?



Proliferation of AI Laws Across U.S.

- Over 160 AI-Specific Laws Enacted
- Through 2025
  - 40% Targeting AI Images / Deepfakes
  - 25% Targeting Government / Campaign Use
  - 20 Automated Decision-Making Laws
  - 9 AI Transparency-Related Laws
  - 2 “Comprehensive” AI Laws – CO & TX
  - Additional Laws for:
    - AI Calling
    - AI in Critical Infrastructure
    - AI Ownership / Liability Presumptions
    - AI in Regulated Industries (Healthcare / Insurance)
    - AI in Social Media

Nearly 1,000 AI-Related Bills Considered in 2025



Source: Orrick’s AI Law Center | U.S. AI Law Tracker

U.S. State AI Law Common Principles

Transparency

Consumers should be informed when interacting with AI or consuming its content.

- CA & ME Chatbot Laws
- IL & NV Mental Health Bot Laws
- NY AI Companion Law
- CA AI Transparency Laws
- Colorado AI Act
- Texas TRAIGA
- Utah AI Consumer Protection

High Risk Restrictions

Consumers should not be exposed to AI content / decisions in higher risk settings w/o proper precautions.

- Colorado AI Act
- Illinois Automated Decision Tools Act
- Illinois Artificial Intelligence Video Interview Act
- New York City Employment Decision Tool Law
- U.S. State Automated Decision-Making Laws

No Discrimination

Consumers should not be subject to discrimination due to bias in artificial intelligence.

- California AI Employment Regs
- Colorado AI Act
- Colorado Insurance Law
- IL Automated Decision Tools Act
- Texas TRAIGA
- U.S. Human Rights Acts

Responsibility

Companies will be held responsible for the acts and mistakes of their artificial intelligence.

- Case Law is Coming
  - Air Canada was held responsible for incorrect disclosures its chatbot provided a consumer in Canada.
- Statutes are Assigning Risk
  - The Utah Artificial Intelligence Policy Act makes users of generative AI generally responsible for the use of their technology.

Global Expansion of AI Regulation

European Union AI Act Takes Effect

The EU AI Act prohibitions on certain types of AI and the AI literacy requirements both went into effect February 2025; and the GPAIM obligations for new models took effect August 2025. Fines for non-compliance with prohibitions can be steep—up to 7% of global annual revenues or €35m, whichever is higher. Enforcement starts in August 2026.

China AI Measures & Nat'l Standards

The Interim Measures for the Management of Generative AI Services came into effect in August 2023 to regulate public-facing generative AI within China. Starting September 2025, new "Labeling Rules" will require AI-generated content to be implicitly labeled, as well as explicitly labeled in certain circumstances. National standards have also been released.

South Korea Ai Framework Act

Effective January 2026, the Act is designed to primarily regulate high-impact AI, generative AI and high-performance AI systems. The Act imposes transparency requirements, labeling requirements for generative AI content, and risk management requirements for certain types of AI systems.

Global Application Of Traditional Laws

Like the U.S., countries are applying traditional laws and legal concepts to AI use cases. For example, Air Canada was held liable for its chatbot giving a passenger incorrect fare-related information in a Canadian court and a court in China held a generative AI platform contributorily liable for copyright infringement of AI output.

U.S. Federal AI Trends

Federal Regulators Take Step Back from AI Policing

FTC Chairman Ferguson allegedly called to "[e]nd the FTC's attempt to become an AI regulator," while other federal agencies are following Trump's call to support AI innovation by narrowing their AI enforcement vision.

Congress Passed the TAKE IT DOWN Act

First significant bipartisan federal AI legislation criminalizes the publication of non-consensual intimate imagery, including AI-generated deepfake images, and requires platforms to remove such content upon request.

Proposed Moratorium on State AI Law Fails

The One Big Beautiful Bill Act incorporated a multi-year moratorium or "pause" on state-level AI enforcement in exchange for certain broadband funds—the AI Enforcement Pause was voted down and removed from the final Bill.

Trump Administration AI Action Plan & Executive Orders Shape Federal Government Focus on AI

The EU AI Act's Risk-Based Approach

Prohibited AI

Prohibits certain AI practices deemed to be unacceptably risky, such as manipulative or deceptive AI.

Effective Feb. 2, 2025

High-Risk AI

Imposes compliance obligations and restrictions on AI systems creating a high risk to the health and safety or fundamental rights of natural persons, such as AI intended to be used for employment decisions.

Effective starting Aug. 2, 2026

Transparency

Imposes transparency obligations on certain AI systems that generally interact directly with individuals or expose individuals to AI-generated content.

Effective Aug. 2, 2026

General-Purpose AI

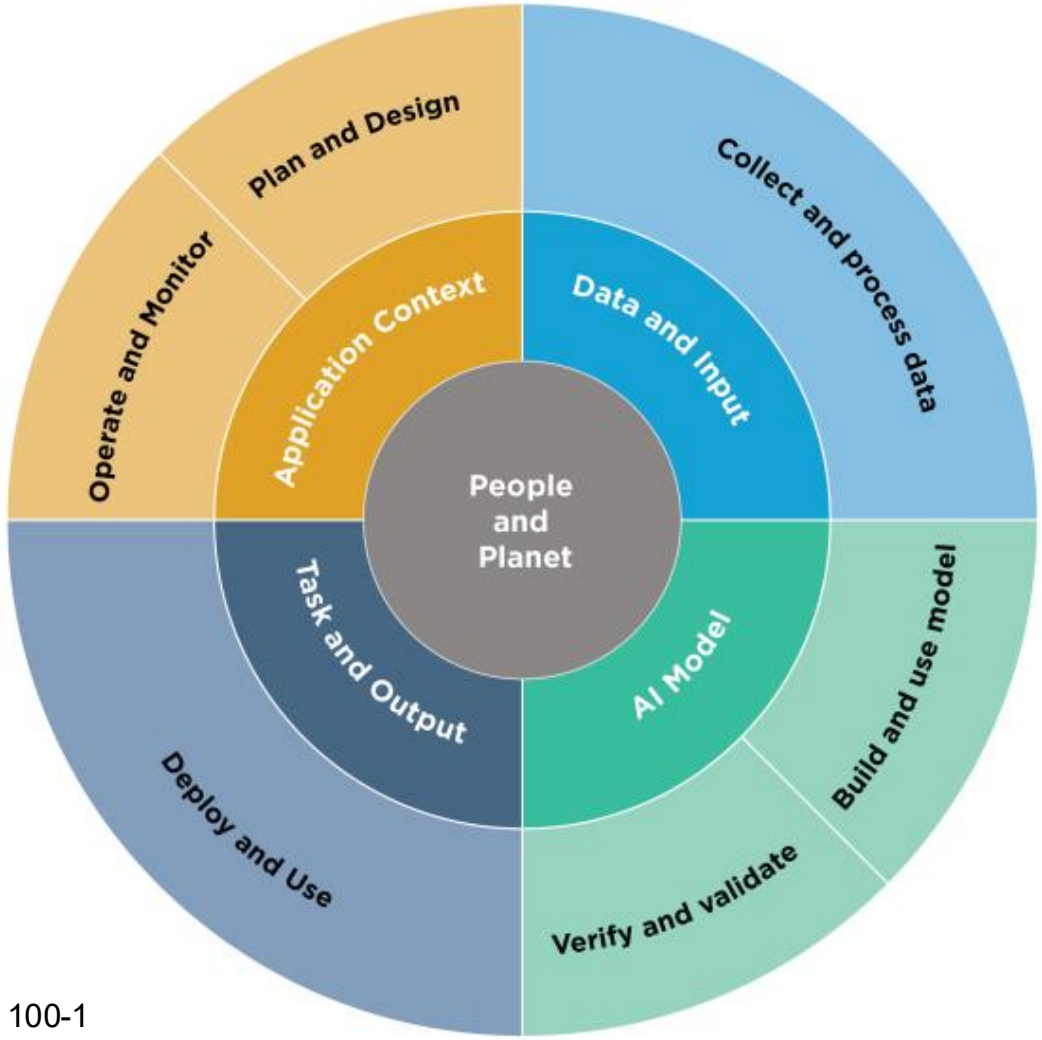
Imposes additional compliance obligations and restrictions on AI models that display significant generality and are capable of competently performing a wide range of distinct tasks, which can be integrated into a variety of downstream systems or applications.

Effective starting Aug. 2, 2026

All other AI systems remain subject to existing legislation/regulation (including GDPR) without additional requirements under the proposed AI Regulation

Industry / Self Regulation of AI

- Self-regulatory frameworks for AI governance:
  - NIST AI Risk Management Framework
  - ISO 42001
  - OECD Framework for the Classification of AI Systems



NIST AI 100-1

Preparing for Litigation & Enforcement

Current Litigation

Wiretap & Privacy Litigation

Plaintiffs counsel aggressively claiming use of AI to facilitate consumer communications and online tracking constitutes unlawful eavesdropping or wiretapping.

Orrick actively defending numerous companies in wiretap litigation.

Courthouse News Service

Google must face claims of AI-powered wiretapping, California judge rules

IP Litigation

Significant ongoing litigation regarding existential issues relating to IP protection in AI training and the limits to fair use and other defenses.

Orrick actively defending Microsoft and other clients in IP-related AI litigation.

Bloomberg Law News

Big Tech Wins in Copyright Cases Come With Strings Attached

Employment Litigation

Emerging groundbreaking legal challenges in the realm of AI and its potential impact on HR-related discrimination and other workplace activities.

Orrick actively defending Workday and others in employment-related AI litigation.

Staffing Industry Analysts

SiriusXM Radio faces class action on AI discrimination

A Detroit-based IT professional filed a class action alleging SiriusXM's AI hiring tool discriminated against African American applicants.

AI Enforcement

Increasing regulatory inquiries and investigations into practices and impacts of AI model developers and deployers under traditional and AI-specific laws.

Orrick actively advising clients on AI-related inquiries and risk assessments.

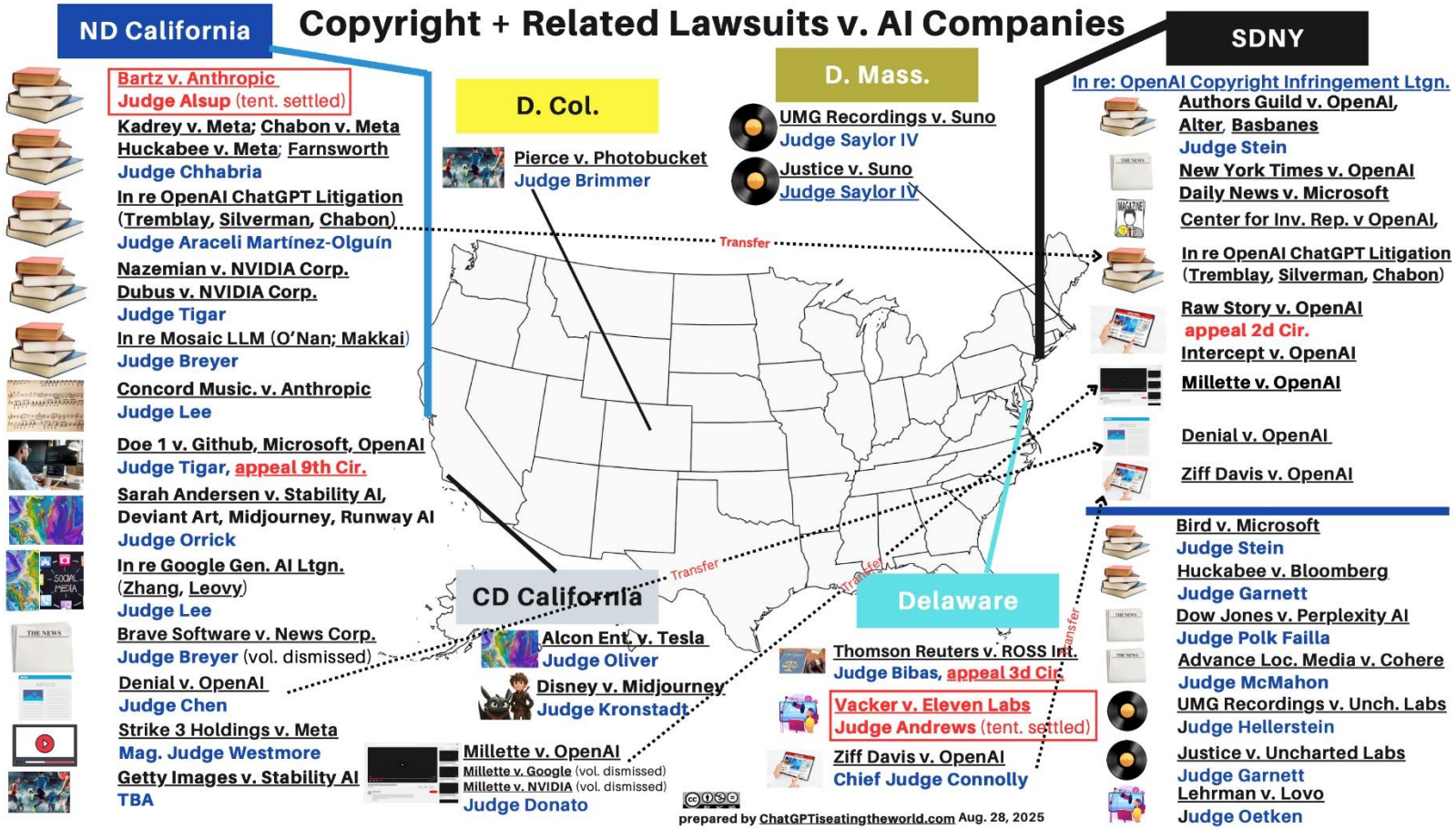
Mashable

44 state attorneys general serve notice to AI companies: Protect our kids — or else

Attorneys general from across the U.S. are warning Big Tech companies about exploiting children with their AI products.

Preparing for Litigation & Enforcement

- One Big Input Question: Is acquisition and use of content for training a fair use?
  - Stakes: No-strings development vs. rights/license-based system
- Countless Little Output Questions: Who/what/when of liability for AI-based products?
  - Stakes: Norms and best practices for mitigating risk in development and use of products



From chatgptiseatingtheworld.com

Examples of U.S. AI Enforcement

Earnest Operations MA AG Settlement

In July 2025, the MA AG's Office announced a $2.5 million settlement with Earnest Operations LLC to resolve allegations that the company's lending practices violated various consumer protection and fair lending laws, including through the use of AI models that could lead to disparate harm to minority applicants and borrowers.

Rytr FTC Order

In September 2024, the FTC announced five law enforcement actions against operations that overused AI hype or sold AI technology that could be used in deceptive and unfair ways.

In December 2024, the FTC approved a final consent order against Rytr, settling allegations that it sold an "AI Testimonial & Review" service that provided subscribers with the means of generating false and deceptive online reviews.

Pieces Technology TX AG Settlement

In September 2024, the TX AG's Office announced a settlement with Pieces Technologies to resolve allegations that the company made a series of false and misleading statements about the accuracy and safety of its generative AI clinical software.

Ongoing Actions & Investigations

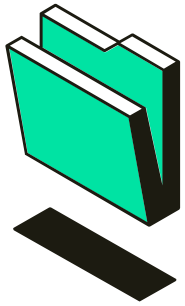
Many ongoing regulatory actions and investigations into AI practices:

- SEC allegations that the founder and former CEO of Nate Inc. made false & misleading statements to investors about Nate's purported AI technology.
- TX AG announced it has opened an investigation into AI chatbot platforms, for potentially engaging in deceptive trade practices and misleadingly marketing themselves as mental health tools.

Top Privacy Challenges

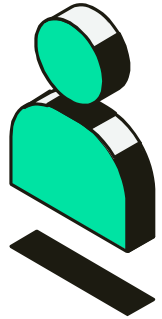
Manual data mapping

Understanding what data exists across the organization remains a massive challenge



Broken assessments

legal requirements now mandate them, but the process is cumbersome and stakeholder-heavy.



Scaling with lean teams

Privacy demands are growing exponentially while team sizes remain flat. Manual processes can't keep up.

Splintered AI governance

Teams know they need AI but face a paradox: agents need data access while privacy demands data minimization.

Building a Privacy-First AI Culture

Building a Strong AI Foundation

How do we develop a culture of responsible AI use without impeding business objectives?

2024

General internal AI use policies

2025

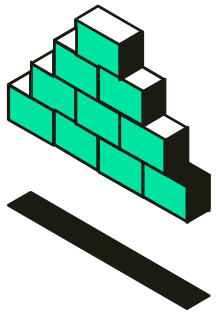
Adjacent policies: production access, meeting transcription, HR tools

2026+

Agent-specific governance, data access frameworks

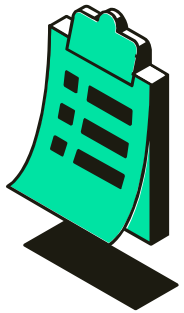
Making AI Work For You at Every Stage of Your Journey

Pre-Requisites



AI Governance Leadership

Cross-departmental Accountability



Purpose-built Policies

1 Adopting

What are quick AI wins and improvements my team can use today?

Admin tasks without PII/SPI	Prompts and no-cost tools	Engage privacy community

2 Scaling

What are time and resource intensive tasks we can automate with AI?

Cookie categorization	Assessment doc review	Privacy page drafts

3 Operationalizing AI Agents

AI agents thrive on context and data access… but privacy demands data minimization.

How do we reconcile these?

Map the datasets the agent will access.

Begin with **read-only actions** and expand permissions as confidence grows.

Contain agents and models internally.

Create specific policies for agent access, transcription tools, and HR tools

More Resources

AI Prompt Library

Try free sample prompts for privacy jobs you can use in GPT, Claude, Gemini, etc.

Get them here

Privacy Slack Community

Join 2k other privacy pros to compare notes in channels like #ai-labs.

Join here

Privacy & AI Newsletter

New resources, articles, and events in your inbox monthly.

Sign up

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/AbBPvZ8HpK

Thank you in advance!

For more information: www.iapp.org

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**