STATE ATTORNEY GENERAL ENFORCEMENT

Privacy, Security and AI Enforcement Report

January – April 2026

Report Period	Bi-Monthly Edition 1
Dataset	307 enforcement actions*

01 Executive Summary

This report covers state AG enforcement activity in privacy, cybersecurity, and artificial intelligence through April 2026, drawing on 307 tracked enforcement activities — including regulatory investigations and actions, regulator sweeps, and stated regulator enforcement priorities.*

Enforcement activities tracked in this report include formal regulatory investigations and actions (*e.g.*, CIDs, consent orders, lawsuits, settlements), regulator sweeps (coordinated multi-target or multi-state enforcement campaigns), and stated regulator enforcement priorities (published guidance, advisories, and formal policy announcements signaling intended enforcement focus areas).

THE ACCELERATION OF AG ENFORCEMENT ACTIVITY SINCE 2022

The regulatory landscape for privacy, information security, and AI is no longer a slow-moving tide — it is a wave, and it is accelerating. State attorneys general (AG) and dedicated privacy regulators (*e.g.,* CalPrivacy) have emerged as one of the most consequential and nimble forces in the enforcement ecosystem, moving faster than federal regulators, responding to constituent pressure, and increasingly coordinating across state lines to pursue companies whose data practices fall short of evolving legal standards.

For legal practitioners and privacy professionals, keeping pace with this enforcement activity is no longer a matter of periodic check-ins or annual reviews - it demands near real-time awareness of where regulators are looking, what conduct they are targeting, and how their theories of liability are evolving. That is precisely what this tracker is built to deliver: a living, continuously updated intelligence resource that ingests state AG settlements and enforcement actions as they happen, and identifies emerging trends before they become widespread. Using this report and more significantly the five years of underlying data we have collected and curated, we can help our clients proactively reduce their regulatory risk and ready them in the event they need to respond to AG investigations or actions.

This inaugural report sets the foundation, providing a historical lens on AG privacy, information security, and AI enforcement activity from 2020 to the present. The numbers show significantly accelerating state AG growth starting in 2022 and continuing to present. If current patterns hold through the end of 2026, we are on pace to see approximately 130 AG enforcement actions this year alone, more than quadruple the 31 recorded in 2022. Will this trend continue? What factors are influencing enforcement activities? With the advent of AI and even more demand for data, are we also in the midst of or entering a materially more risky regulatory enforcement environment?

These are the core questions we are exploring with our AG tracker — we will do so using both the data we've gathered and aggregated in this report using AI and our vast AG and privacy compliance experience our team has obtained over decades.

KEY FINDINGS

+52%
Year-Over-Year Enforcement Growth

2025 saw 99 actions — up 52% over 2024's 65. At current pace, 2026 projects to ~130.

See Historical Overview →

43
2026 Actions YTD

43 actions filed Jan–Apr 2026, including major AI enforcement and multistate coalitions.

See Period in Review →

12
AI Actions in 2026 YTD

AI enforcement continues its surge: 14 actions in 2025 (up 56% from nine in 2024), with 12 already in 2026 through April.

See Category Breakdown →

$195.8M
Non-Outlier Settlement Baseline

Excluding mega-settlements, 51 actions produced $195.8M — the real enforcement cost baseline for most companies.

See Settlement Analysis →

ANALYSIS AND GUIDANCE

Insights and Trends
What the data tells us

AI enforcement acceleration, multistate coalition expansion, and Privacy as the dominant enforcement vector.

Read Analysis →

Response and Defense
How to respond when it happens

Resolution patterns, multistate defense coordination, and practical response considerations.

Read Defense Dynamics →

Compliance Corner
What to do proactively

AI governance, children's data audits, data broker monitoring, and multistate preparedness.

Read Guidance →

02 Historical Overview

Cumulative enforcement trends since the dataset's earliest entries. Action volume, category distribution, geographic concentration, and year-over-year momentum.

Total Actions Tracked
307
Since 2020 · Primary growth since 2022*

2026 YTD Actions
43
Proj. ~130 annualized

Total Settlements
$5.52B
63 resolved actions

Excl. Outliers
$195.8M
51 non-outlier settlements

Multistate Actions
77
25% of all actions involve 5+ states

FROM DATA SECURITY TO PRIVACY ENFORCEMENT

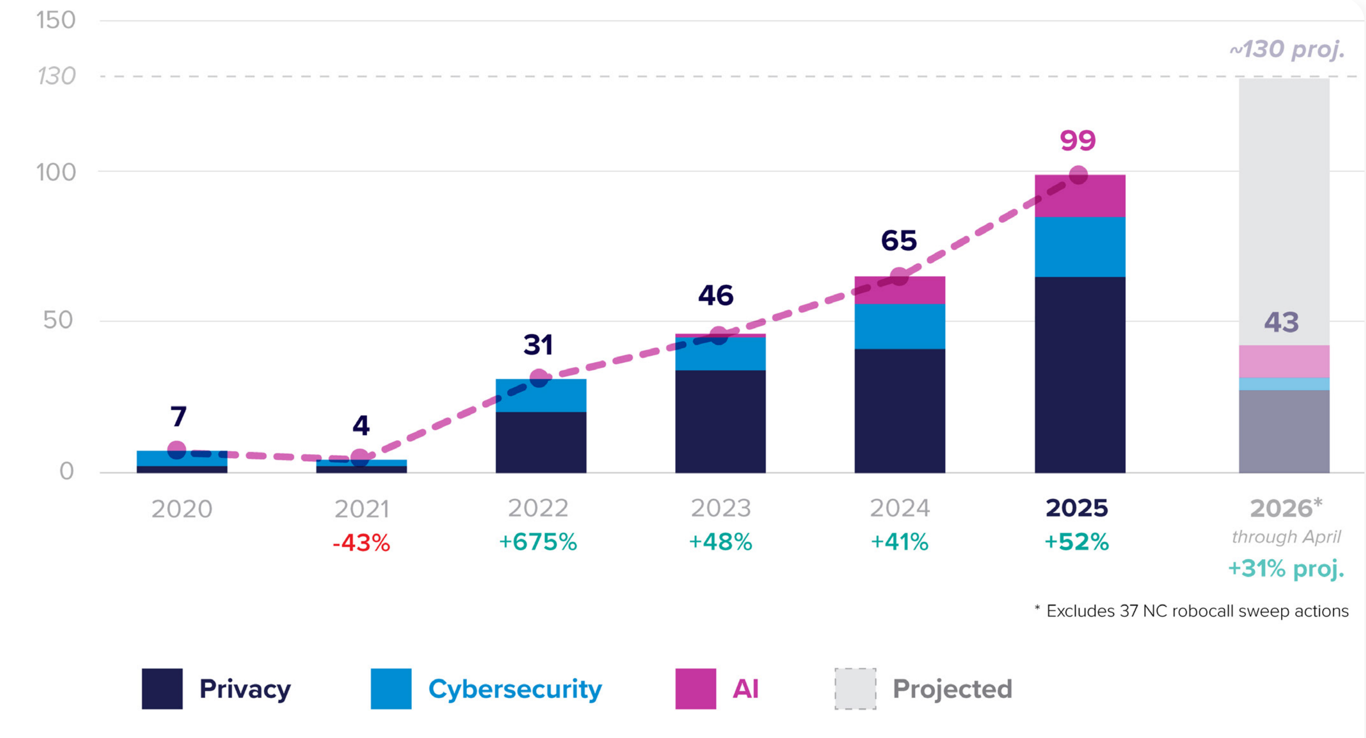
Since 2022, state enforcement activity related to cybersecurity, privacy, and artificial intelligence has accelerated dramatically. This surge is not a coincidence: it reflects years of deliberate planning, coordination, and capacity-building among state regulators, who now bring deeper subject-matter expertise and a more sophisticated understanding of emerging technologies.

In a landscape of rapid technological change, states have recognized that they are uniquely positioned to move faster than their federal counterparts. Leveraging broad authority under state unfair and deceptive acts and practices (UDAP) laws, state AGs have stepped into a more prominent enforcement role—particularly as shifting federal priorities and deregulation efforts have created a perceived enforcement gap. Beyond the increased expertise of the AGs, the question remains: what motivates state AGs and privacy regulators to enforce on a particular issue at a particular time? We will explore that issue in future iterations of this report.

The data shows a clear inflection point beginning in 2022. Historically, state AG privacy and cybersecurity enforcement focused largely on data breach incidents. Today, with heightened regulatory sophistication and specialized technical expertise, state enforcers are increasingly scrutinizing companies' day-to-day privacy practices and the potential for consumer harm well beyond the context of a data breach. This evolution has transformed the state regulatory landscape into a powerful, proactive force that companies must navigate strategically.

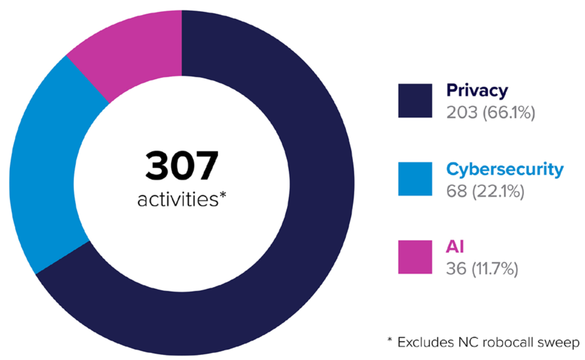
ACTIONS BY YEAR (STACKED BY CATEGORY)

YoY% change shown • 2026 data through April • Projection based on YTD run-rate



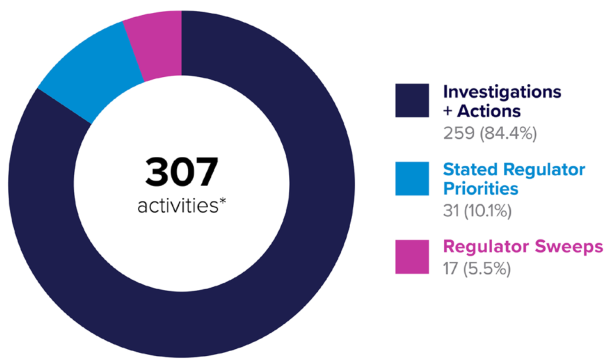
ACTIONS BY CATEGORY (ALL TIME)

Distribution across 307 enforcement actions*



ENFORCEMENT ACTIVITY TYPE

Classification of tracked enforcement activities



TOP 10 MOST ACTIVE STATES

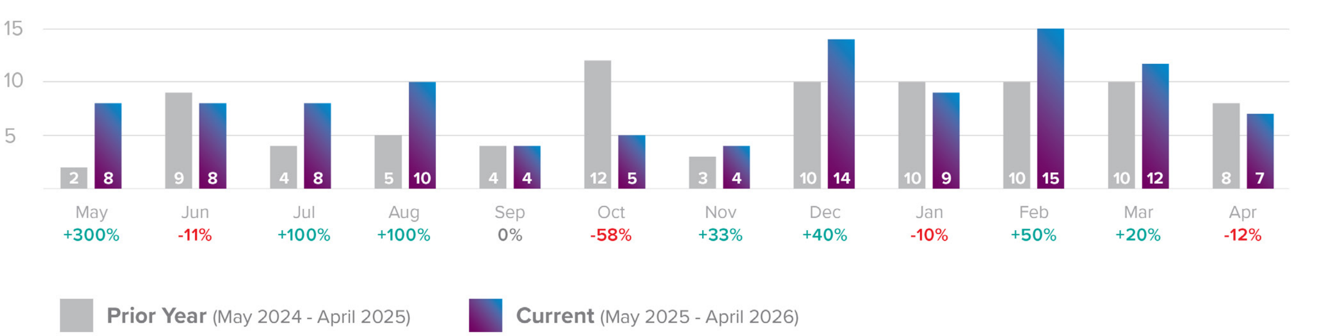
By number of actions initiated (as lead state)*

State	Actions
California	32
New York	26
North Carolina	24
Texas	19
Connecticut	11
Oregon	11
West Virginia	11
Pennsylvania	10
Oklahoma	9
Hawaii	8

MONTHLY ACTIONS: 12-MONTH LOOKBACK (YEAR-OVER-YEAR)

Current (May 2025 - April 2026) vs. prior year (May 2024 - April 2025)

Total: 104 vs. 87 (+20%)



03 Period in Review

New enforcement actions filed during the current reporting period (January–April 2026).

A BUSY BEGINNING OF 2026

The first third of 2026 has seen explosive settlements by state AGs and privacy regulators in privacy, cybersecurity, and artificial intelligence. These settlements highlight the growing enforcement power and rapidly evolving legal landscape. For example, the California AG announced a record $12.75 million settlement with a large automotive company for allegedly selling location and driving behavior data without adequate notice or consent, in violation of the California Consumer Privacy Act. The settlement included not only the monetary penalty but also strict requirements for improved consumer disclosures and opt-out mechanisms.

In Alabama, the AG secured a $12.2 million settlement with a major interactive gaming platform over child safety and privacy concerns. The injunctive relief was particularly robust, mandating age verification using facial estimation and government ID, expanded parental controls, and restrictions on communications involving minors.

Additionally, Massachusetts reached a $515,000 settlement with a billing vendor, for a data breach affecting sensitive patient information. The injunctive relief required ongoing independent security assessments and enhanced security measures.

These settlements underscore the trend toward higher monetary penalties and increasingly detailed injunctive relief, reflecting the heightened expectations for compliance, transparency, and proactive risk management in the evolving regulatory landscape of privacy, cybersecurity, and AI. What will be interesting, and a topic of future reports, is comparing the impact of the financial settlements against the costs and organizational changes tied to injunctive relief. We often focus on the former when the latter may be more challenging for many organizations to address.

NEW ENFORCEMENT ACTIVITIES THIS PERIOD

43 enforcement activities filed January–April 2026 · Full list in Appendix A →

Total This Period	Investigations and Actions	Stated Priorities	Regulator Sweeps	Settlements
43	**27**	**12**	**4**	**$560K**
Jan–Apr 2026	Named defendants	Guidance, advisories and AG coalition statements	Industry-wide actions	2 actions with monetary outcomes

04 Enforcement by Category

Three-level enforcement taxonomy with a one-to-one relationship between categories. Each L3 tag belongs to exactly one L2 subcategory under one L1 category.

PRIVACY ENFORCEMENT STILL PRIORITIZED, BUT AI ENFORCEMENT IS HERE AND GROWING

We've organized our analysis of state privacy enforcement into three broad categories: (1) privacy; (2) cybersecurity; and (3) AI. Within each category, state AGs and privacy regulators investigate and enforce on a variety of topics. You can cycle through the historical landscape below and identify the exact areas regulators are targeting and slice the data in a variety of manners.

State privacy enforcement is rapidly becoming a substantial regulatory priority for regulators, as evidenced by a dramatic increase in such actions over the past five years. Regulators are moving beyond traditional data breach actions focused on privacy, including how organizations collect, use, and share personal information in real time.

Artificial intelligence (AI) represents a newer regulator priority, but it is the fastest growing enforcement category. Interestingly, unlike privacy enforcement where there was a significant lag between certain data processing activities and enforcement, it appears state AGs and privacy regulators are attempting to stay on top or get ahead of enforcement on AI issues. To the extent enforcement helps set the legal "guardrails" around the use of AI, state regulators arguably play a frontline and outsized role in the development and use of this technology.

What the data shows, and we expect going forward, is a substantial increase in AI enforcement (with some overlapping privacy issues involved), as regulators gain a deeper understanding of how the technology is deployed by the industry, develop institutional expertise and inter-agency working groups focused on AI, and as states adopt new laws specifically governing AI in consumer-facing contexts.

PRIVACY (203 ACTIONS)				
Data Type / Subject-Matter Privacy (122)				
Children's / Minor Data **78**	Geolocation / Precise Location Data **21**	Genetic / Health Data **16**	Financial / Identity Data **14**	Biometrics **12**
Core Privacy Governance / Compliance (118)				
Notice / Transparency **70**	Data Governance **62**	Data Sharing / Sale / Targeted Advertising **49**	Consumer Rights / Request Handling **39**	Vendor Management / Service Provider Controls **4**
Market-Specific / Business Model Privacy (102)				
Social Media / Platform Data Practices **60**	Adtech / Online Tracking / Pixels / SDKs **19**	Data Brokers / Aggregation **16**	Connected Devices / IoT Privacy **16**	
Communications Privacy (33)				
Robocalls / Telemarketing / TCPA-Type Conduct **31**	Caller ID / Spoofing / Lead Generation **10**	Email Marketing / CAN-SPAM-Type Conduct **1**		
CYBERSECURITY (68 ACTIONS)				
Incident-Focused (62)				
Data Breach **47**	Unauthorized Access / Intrusion **44**	Incident Response / Notification Failures **15**	Ransomware **7**	
Security Program / Controls (57)				
Information Security Program Deficiencies **53**	Access Controls / Identity and Authentication **23**	Governance / Board Oversight **18**	Third-Party / Vendor Security **8**	
Sector- or Data-Specific Security (17)				
Genetic / Health Data **12**	Children's Data Security **2**	Critical Infrastructure / OT **1**		
ARTIFICIAL INTELLIGENCE (36 ACTIONS)				
AI Governance / Lifecycle (27)				
AI Governance / Risk Management **17**	AI Transparency / Disclosure **12**	Synthetic Media / Provenance / Labeling **11**	AI Safety / Model Safety **3**	
AI Misconduct / Enforcement Theories (22)				
Unfair or Deceptive AI Practices **13**	AI-Enabled Fraud / Scams / Manipulation **11**	Automated Decision-Making **3**		
AI Use-Case / Harm Area (16)				
Chatbots / Consumer-Facing AI Assistants **6**	Algorithmic Bias / Discrimination **4**	Health Care AI Applications **1**	Government / Law Enforcement AI **1**	
AI Security / Misuse (1)				
Cyber Misuse / Offensive Use **1**				

Each enforcement activity belongs to one Level 1 Category, with one or more Level 2 Subcategories and Level 3 Tags assigned within that category · L3 tags have a one-to-one relationship with their L2 Subcategory

05 Settlement Analysis

Financial outcomes of AG enforcement. 63 of 259 investigations and actions (24.3%) resulted in monetary settlements.* Outlier settlements are defined as those ≥$40M (12 actions, 96% of total settlement dollars) and are analyzed separately to reveal the typical enforcement baseline.

LOOKING BEYOND THE HEADLINES: DAY-TO-DAY SETTLEMENTS AND ENFORCEMENT PRIORITIES

High-profile settlements — such as actions against big tech, large multistate resolutions, or matters heavily covered in the press — offer useful context, but they may skew the state AG and privacy regulator settlement landscape. These headline cases are often outliers, with penalties that far exceed the amounts regulators typically pursue in the ordinary course. They do serve an important role for signaling regulator priorities and identifying practices that organizations may need to address to avoid legal risk.

Nonetheless, the real insight lies in the routine, day-to-day settlements that are much harder to find, collect, and analyze. Those “ordinary” settlements are where regulatory expectations (beyond the headlines) are most clearly expressed and where the practical boundaries of the law are set. Understanding the dollar values achieved, the injunctive terms imposed, and how regulators apply state-specific statutes in these matters gives companies concrete, data-driven benchmarks. With this information, organizations can negotiate more effectively with regulators, anticipate areas of emerging focus, and align their compliance programs with what enforcement agencies are actually doing.

We’ve got all the data and have crunched it below. We use these insights not only for this report, but for our on-the-ground advice to clients facing state AG and privacy regulatory enforcement — understanding regulators’ specific patterns gives our clients a leg up.

Total Settlement Dollars
$5.52B
63 actions with payments

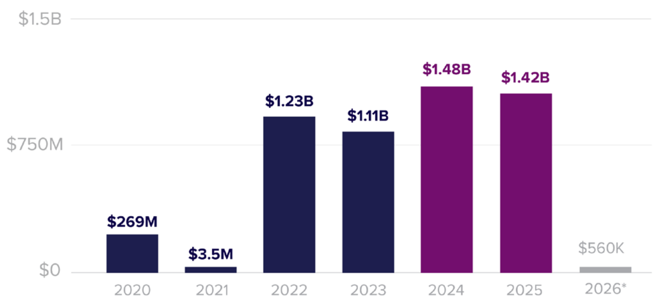
Outlier Settlements
$5.32B
12 actions (96% of total $)

Non-Outlier Total
$195.8M
51 actions — the baseline

No Payment
196
76% of investigations and actions

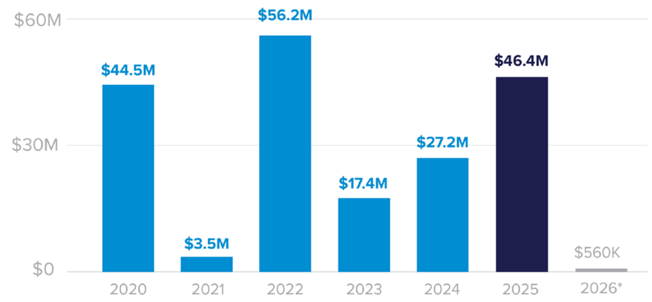
TOTAL SETTLEMENT PAYMENTS BY YEAR

Includes all settlements • Outliers dominate 2022-2025



SETTLEMENT PAYMENTS — EXCLUDING OUTLIERS

51 non-outlier settlements reveal the typical enforcement baseline



2025 non-outlier settlements: highest on record

SETTLEMENT CENTRAL TENDENCIES

Average and median reveal the gap between headlines and typical exposure

All Settlements (n=63)

Average	Median
$87.5M	**$1.2M**

73× gap between mean and median — driven by 12 outlier settlements (≥$40M each)

Excluding Outliers (n=51)

Average	Median
$3.8M	**$530K**

This is the realistic enforcement baseline for most companies

Why this matters: The 73× gap between the all-in average ($87.5M) and the all-in median ($1.2M) shows how dramatically a handful of mega-settlements against two major technology companies and a credit reporting agency distort the picture. For the typical company facing AG enforcement, a median settlement of **$530,000** (excluding outliers) is a far more relevant planning number than the headline-grabbing billion-dollar figures.

06 Industry Targets

Industry classification based on NAICS sector codes assigned to each defendant in the dataset.

INDUSTRY-LEVEL DATA AND DRILL-DOWN INSIGHTS

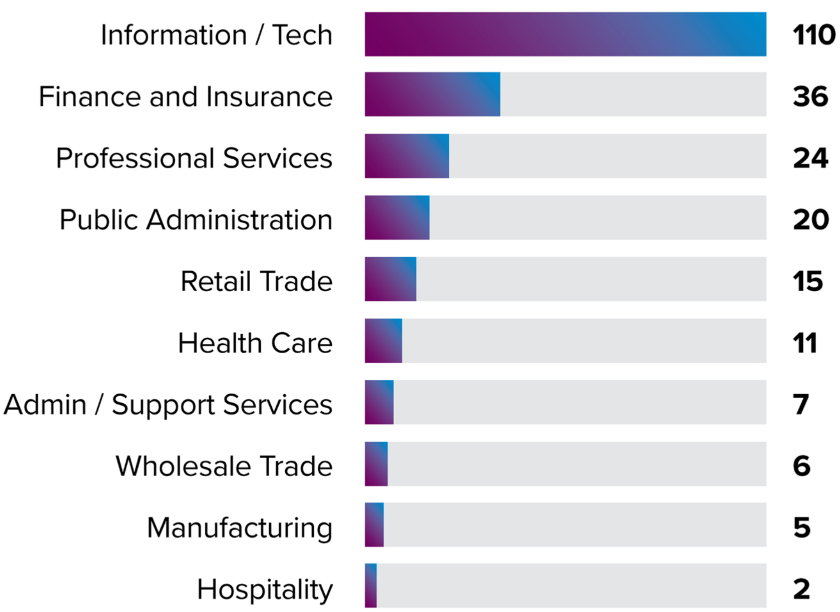
We continuously collect and analyze state AG and privacy regulator settlements and classify them by industry, giving organizations a clear, data-driven view of regulators' priorities.

Understanding which sectors are in the crosshairs of regulatory scrutiny is critical for assessing compliance risk and making informed decisions about enforcement response and compliance budgeting. Our data analysis drills down further into the specific issues regulators are prioritizing by industry and the states that are most active in pursuing them.

Armed with this intelligence, companies operating in higher-risk industries can develop informed risk-based compliance decisions, strategically plan their operations and product and service offerings, and navigate regulatory expectations with greater confidence.

ACTIONS BY INDUSTRY (NAICS SECTOR)

Top 10 industries by enforcement action volume



SETTLEMENT STATISTICS BY INDUSTRY (EXCL. OUTLIERS)

Average and median settlements by NAICS sector · Industries with 2+ settlements

INDUSTRY	ACTIONS W/ $	AVERAGE	MEDIAN	TOTAL
Finance and Insurance	11	**$9.4M**	**$3.0M**	$103.4M
Information / Tech	7	**$6.6M**	**$515K**	$46.5M
Real Estate	2	$3.9M	$3.9M	$7.8M
Professional Services	6	$2.0M	$350K	$12.1M
Retail Trade	7	$1.5M	$345K	$10.4M
Health Care	8	$1.2M	$498K	$9.5M
Wholesale Trade	3	$950K	$500K	$2.9M
Admin / Support Services	4	$56K	$48K	$224K

Sorted by average settlement amount · Outlier settlements (≥$40M) excluded to show typical exposure

07 Privacy Focus

Privacy enforcement actions during the current reporting period (January–April 2026). 27 of 43 period actions (63%) are privacy-related — the dominant enforcement category by volume. Full list in Appendix A →

PRIVACY ENFORCEMENT IS STILL THE KING AND STILL ACCELERATING

By volume, privacy enforcement has dominated other enforcement categories since 2022, and that trend continued in the first four months of 2026. With 23 states now having passed comprehensive consumer privacy laws, state AGs and privacy regulators are now actively reshaping compliance obligations through enforcement across every industry. The stark reality for all businesses is that privacy regulators are organized, motivated, focused and funded (through large settlements and legislative mandates) for impactful privacy enforcement.

The picture painted by the data shows a maturing enforcement approach that utilizes a combination of sweeps, investigations and enforcement actions to highlight priorities and drive compliance in the privacy space. Understanding the data and trends is a necessity for companies seeking to deploy risk-based positioning for privacy compliance. The risk here is more crucial for a multitude of companies seeking to leverage personal information and implement AI-fueled data strategies tied to personal information.

Children's data protection has emerged as a top enforcement priority, with high-profile actions highlighting that platforms serving younger audiences face heightened scrutiny and significant legal exposure. At the same time, connected device privacy has emerged as a critical new enforcement vector, illustrating that the regulatory gaze has expanded well beyond traditional app and web ecosystems. Data broker regulation is also taking concrete shape, with meaningful enforcement activity in New York, Alabama, and California establishing the compliance benchmarks that businesses handling consumer data must now meet. With California's DELETE Act coming online, and new laws like Connecticut's Data Broker Act, we expect to see a material increase in enforcement in this space, including against companies who may not consider themselves traditional data brokers.

Meanwhile, the broadening of consumer rights enforcement - driven by new and revised privacy laws, including Oregon's Global Privacy Control requirements and Alabama's Data Protection Act - means that companies operating across state lines must navigate an increasingly complex and fragmented legal landscape. Taken together, these developments underscore the urgency of proactive privacy compliance strategies and the value of counsel with deep expertise at the intersection of regulatory enforcement and emerging technology.

Privacy Actions
27
Jan–Apr 2026 · 63% of period total

All-Time Privacy
203
66.1% of all 307 actions

YoY Trend
+59%
2024 (41) → 2025 (65)

Top Tag
Children's Data
10 tags this period · 78 all-time

EMERGING ENFORCEMENT THEMES

Period L3 tag distribution — Privacy enforcement areas active in Jan–Apr 2026

Children's / Minor Data	**10**
Data Governance	**10**
Notice / Transparency	**10**
Consumer Rights	**6**
Platform Data Practices	**5**
Data Sharing / Sale	**5**
Financial / Identity Data	**4**
Connected Devices / IoT	**4**
Data Brokers	**2**
Genetic / Health Data	**2**

08 Information Security Focus

Cybersecurity enforcement actions during the current reporting period (January–April 2026). While only 4 actions this period, they signal expanding scrutiny of security program adequacy beyond traditional data breach response.

Full list in Appendix A →

REGULATORY SECURITY PROGRAM SCRUTINY - POST- AND PRE-DATA BREACH

The era of waiting for a data breach to spark regulatory scrutiny of a company's cybersecurity program is over. For decades, cybersecurity enforcement was a creature of hindsight — state AGs descending on companies only after the damage was done. That paradigm is beginning to erode. While regulators still scrutinize data breach response, they increasingly focus on potential security program deficiencies that resulted in a breach. This is reflected in their investigations, as well as in settlements that include mandates to build appropriate security programs and implement specific controls. These mandates are accompanied by risk assessment, monitoring and reporting requirements that can span years.

From a compliance and risk-reduction point of view, companies should re-address "legally defensible" security and ensure the story behind their security program and the choices they made resonate in front of an AG or privacy regulator. The enforcement focus on the adequacy of an organization's security program (even when a breach has not occurred) is likely to increase. For example, CCPA regulations require qualifying businesses to complete an annual, independent cybersecurity audit documenting their security program—including any identified gaps or weaknesses. A member of executive management must then certify, under penalty of perjury, that they reviewed and understood the audit, and the business must submit an annual certification of completion to CalPrivacy. The result is a signed, sworn, contemporaneous record that regulators can scrutinize—well before any breach occurs. These back-end documentation requirements are bound to lead to more information security-related sweeps, investigations and enforcement actions.

Cyber Actions
4
Jan–Apr 2026 · 9% of period total

All-Time Cyber
68
22.1% of all 307 actions

YoY Trend
+33%
2024 (15) → 2025 (20)

Top Tag
Security Program
3 of 4 period actions cite deficiencies

Proactive Program Scrutiny

Three out of four cybersecurity actions this period target **security program deficiencies** without a preceding breach — a departure from the historically breach-driven enforcement model. These actions signal AG willingness to challenge security adequacy of consumer technology products proactively. This will likely increase as companies are required to certify security compliance under the CCPA.

IoT and Critical Infrastructure

AG enforcement has extended into connected device and network infrastructure security — territory traditionally occupied by federal regulators. Tags include critical infrastructure/OT, governance/board oversight, and third-party vendor security.

09 AI Focus

Artificial intelligence enforcement actions during the current reporting period (January–April 2026). With 12 actions — already approaching 2025's full-year total of 14 — AI is the fastest-growing enforcement category.
Full list in Appendix A →

PROACTIVE AI ENFORCEMENT

The age of AI accountability has arrived, and this time accountability is trying to keep pace. The coalition of 57 states and U.S. territories targeting a well-known AI company stands as a watershed moment, a thunderclap signal that no AI company – regardless of size or valuation – is beyond the reach of state regulators. AGs across the U.S. are not waiting for the federal government to take the lead. State regulators are wielding traditional civil rights, privacy, and consumer protection statutes as powerful tools. The reach of those tools is remarkable.

AI regulatory enforcement now cuts across privacy law, antitrust, state licensing regimes, cybersecurity, intellectual property, and national security laws. A company's use of AI can subject it to the full spectrum of regulatory scrutiny.

On the legislative front, lawmakers in 45 states have introduced over 1,500 AI-related bills, producing a sprawling, fast-moving patchwork of compliance obligations tailored to health care, employment, algorithmic pricing, and child safety. For companies deploying AI in any capacity, the message from state regulators is clear: they are focusing resources on AI enforcement and compliance at a rapidly increasing cadence (and this is true whether or not AI laws ultimately pass).

AI Actions

12

Jan–Apr 2026 · 28% of period total

All-Time AI

36

11.7% of all 307 actions

YoY Trend

+56%

2024 (9) → 2025 (14)

2026 Pace

~36

On track to nearly triple 2025

REGULATOR SWEEPS AND STATED PRIORITIES

Published guidance, advisories, and AG coalition statements signaling AI enforcement priorities

DATE	STATE	ACTION
Apr 2	Oregon	AI governance / risk management guidance, AI transparency
Mar 31	42-State AG Coalition	Letter to Congress backing AI chatbot safety / warning labels for social media platforms
Mar 24	New Mexico	AI governance priorities — government / law enforcement AI focus
Mar 17	Pennsylvania	Consumer-facing AI chatbot safety guidance
Mar 12	Pennsylvania	AI transparency, synthetic media / deepfake enforcement priorities
Feb 27	Pennsylvania	AI governance, deceptive AI practices enforcement framework
Jan 15	New Mexico	AI industry guidance — governance, synthetic media, fraud
Jan 13	Arkansas	AI governance / risk management priorities

Massive Multistate Coalitions

The three largest coalitions in the entire dataset are all AI actions from this period, including coalitions involving 57, 42, and 36 states and territories. AG offices are using coalition size as a force multiplier to signal unified enforcement intent on AI.

Synthetic Media and Deepfakes

Four out of 12 AI actions this period involve synthetic media, provenance, or labeling — making it the second most common AI tag after governance. A multistate action against a social media company and multiple state guidance documents target AI-generated content without adequate disclosure.

State Frameworks Proliferating

Seven out of 12 AI actions are published guidance, advisories, or enforcement framework announcements — AGs are building the enforcement playbook in real time. Pennsylvania alone issued four AI-related enforcement signals this period.

10 Insights and Trends

Analytical observations from the current dataset (307 actions through April 2026).*

WHAT ARE WE SEEING IN THE DATA?

Regulatory intelligence turns regulatory activity from a reactive fire drill into a strategic asset that enables proactive risk assessment and mitigation while enabling organizations to meet their business objectives. By distilling how particular regulators have actually behaved in comparable matters—what they prioritize, how they negotiate, and where they have shown flexibility— companies can approach investigations and supervisory inquiries with a jurisdiction-specific game plan rather than guesswork. That insight allows businesses to narrow overbroad demands, calibrate a credible negotiation posture using historical metrics, and craft narratives that speak directly to the concerns regulators have already signaled.

Allowing companies to lay the foundation for their strategy in data, while leaning on lawyers with deep knowledge and personal relationships with regulators, can materially influence the outcome of an enforcement action or shape a successful compliance campaign.

Just as important, these insights translate into practical, forward-looking risk reduction. Understanding enforcement patterns and outcomes that are relevant to a company's privacy, cybersecurity, and AI practices helps clients understand what regulators care about and where they are actually drawing the line—on consent flows, opt-outs, security controls, breach notification, and automated decision-making. That gives companies a clear blueprint for where to invest first, how to "pressure-test" policies and systems before they are under a microscope, and how to build AI governance that anticipates emerging theories of liability. Most importantly: it enables our clients' business plans, products and services to succeed while taking on a better-measured and appropriate amount of risk.

In an environment where state enforcement is expanding and expectations are evolving quickly, using the insights derived from the data and our expertise means a company is not simply compliant on paper; it is operationally aligned with what regulators are doing in the real world, strengthening its defenses and reducing regulatory exposure in near real time.

AI Enforcement Accelerating

AI actions grew from nine in 2024 to 14 in 2025 (+56%). 2026 already has 12 through April — pacing well above full-year 2025. AI Governance and Deceptive AI Practices are the leading enforcement theories.

Multistate Coalitions Growing

77 actions (25%) involve five or more state AGs acting in concert. Multistate actions have grown from three in 2020 to 31 in 2025, representing a 10x increase in coordinated enforcement.

Privacy Dominates Enforcement

Privacy actions represent 203 of 307 total actions (66.1%), dwarfing Cybersecurity (22.1%) and AI (11.7%). Within Privacy, Children's Data (78 tags), Notice/Transparency (70), and Platform Data Practices (60) are the highest-volume enforcement areas.

11 Response and Defense Dynamics

How enforcement actions unfold, how companies respond, and what defense strategies the data reveals. This section tracks resolution patterns, multistate coordination mechanics, and the practical realities of AG investigations.

DIVING INTO AND USING THE DATA AND INSIGHTS

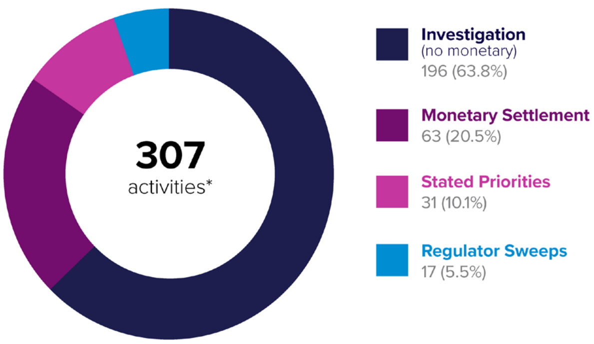
Understanding the broader regulatory landscape helps a company anticipate when an issue is likely to draw attention from multiple jurisdictions, anticipate multistate activity, and align current defense with global strategic goals aimed at protecting the company from risks lurking around the corner. Regulatory intelligence gives decision-makers a clear, data-backed view of exposure and options.

Regulatory intelligence is also critical to defending against an enforcement action because it closes the information gap between the company and the state AG office by showing how the specific regulators who issued the CID have handled similar issues, industries, and fact patterns in past matters. It informs the initial strategy and response efforts by helping frame what the investigation is really about, guiding triage, and supplying precedent-based arguments to narrow scope, timing, and burden. It also shapes the substantive defense narrative and settlement posture by benchmarking theories of liability, remedies, penalties, and remediation that AG offices have actually accepted in settlement.

The data we've gathered, organized and aggregated (from hundreds of disparate sources) is largely unavailable in the market. Its availability is an opportunity: in-house counsel should dive into the data and determine how it can best be deployed to help their companies reduce risk and achieve their business objectives. The use of AI and data, in conjunction with experienced counsel, provides for new opportunities that weren't available before.

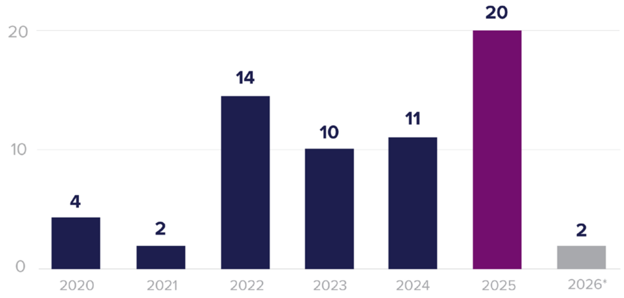
RESOLUTION PATTERNS

How tracked enforcement activities resolve · 24.3% of investigations and actions involve monetary settlement



SETTLEMENT VELOCITY

Annual count of actions resolved with monetary settlement · Indicates pace of resolution activity



Monetary Settlements by Year of Action Initiation
2025 marks peak settlement velocity - 20 actions resolved with monetary outcomes

Why this matters: The dominant resolution path is an investigation or action that closes without a monetary settlement — often via consent order, injunctive relief, or non-financial agreement. Companies that focus only on dollar exposure miss the operational cost of injunctive remediation, which can span years.

Note on methodology: The dataset captures action initiation dates and monetary outcomes but not closure dates, so a strict "duration to resolution" metric isn't computable. This chart instead shows the year-over-year pace of monetary settlements, which is the best available proxy for resolution velocity and signals where AG enforcement is converting from investigation to outcome.

CID Response Strategy

A civil investigative demand (CID) is the first — and often most consequential — inflection point in AG enforcement. Early decisions on scope objections, privilege assertions, and the framing of voluntary submissions shape the trajectory of the entire investigation. The data suggests companies that engage substantively in the CID phase — using regulatory intelligence to anticipate the AG's theory of the case, narrow overbroad demands, and offer credible compliance narratives — are more likely to resolve matters without a formal action or with significantly narrowed injunctive relief. Conversely, reactive or formulaic CID responses tend to harden AG positions and expand the scope of subsequent enforcement. Practical strategy includes assessing multistate exposure early (CIDs frequently coordinate across jurisdictions), preserving evidence and legal hold posture, and treating the CID as a vehicle for a strategic dialogue rather than a discovery exchange.

Multistate Defense Coordination

With 77 multistate actions in the dataset, companies must prepare for coordinated investigations. Lead AG dynamics and achieving global resolution are critical defense considerations.

Settlement Economics

The median non-outlier settlement creates meaningful but manageable exposure. 76% of investigations and actions result in no monetary payment, suggesting that compliance posture and early engagement significantly affect outcomes. The real cost often lies in injunctive relief and ongoing compliance obligations.

12 Compliance Corner

Practical takeaways from the data.

DATA ENABLES BETTER COMPLIANCE CHOICES

Data privacy, security, and AI compliance is complex, ambiguous, and a moving target. Regulator enforcement, litigation, and legislative trends all influence and clarify compliance. Achieving more visibility and insights using AI and data is the natural evolution of risk-based compliance advice. The key compliance corner takeaway for this edition is to determine how detailed AG privacy, security and AI enforcement data can be used to proactively address compliance issues in your organization.

The data we've developed can reduce the guesswork around compliance. Risk-based advice can be provided based both on a lawyer's experience in the space, but also by the insights tied to AI-fueled data analytics. This helps companies' legal teams craft legal compliance positions (especially in gray zones) while supplying business decision makers with better informed risk assessments. Data analysis provides stakeholders with greater confidence to pursue business objectives with more certainty as to the risks they are accepting.

The compliance implications below are drawn directly from patterns in the enforcement data. Each recommendation maps to a specific trend documented in the preceding sections. Regulatory settlements and injunctive provisions are one of the clearest windows into how enforcement agencies actually interpret and apply the law in practice. State AGs routinely use settlements to spell out what they view as unlawful conduct and what they expect from companies going forward, often in far more detail than statutes or regulations themselves.

REVIEW AI GOVERNANCE FRAMEWORKS

With 26 AI enforcement actions in 2025–2026 alone, companies deploying generative AI, automated decision-making, or consumer-facing AI assistants should audit compliance against emerging AG enforcement theories — particularly AI transparency, deceptive practices, and synthetic media labeling.

AUDIT CHILDREN'S DATA PRACTICES

Children's/Minor Data appears in 78 actions across the dataset. Platform safety, COPPA-adjacent practices, and social media data collection remain top enforcement priorities. A 57-state/territory AG coalition signals the broadest coordinated action yet on AI safety for minors.

MONITOR DATA BROKER AND ADTECH EXPOSURE

Data broker/aggregation tags appear in 16 actions, with adtech/tracking in 19 more. New state registration requirements and data sharing enforcement are expanding scope. Companies should assess whether their data practices trigger broker classification.

PREPARE FOR MULTISTATE INQUIRIES

25% of enforcement actions involve five or more states. Companies receiving a CID from one AG should anticipate multistate interest. Develop response playbooks for coordinated investigations — the average multistate coalition in 2025–2026 involves increasingly larger groups of participating offices.

A Appendix A — List of AG Actions

All 43 enforcement activities filed January–April 2026, organized by type.

INVESTIGATIONS AND ACTIONS (27)

Generic entity descriptions for regulatory investigations, enforcement actions, consent orders, and lawsuits against business defendants.

DATE	ENTITY TYPE	CATEGORY	LEAD STATE	STATES	SETTLEMENT
Apr 24	Online Prediction Markets	Privacy	Maryland	1	—
Apr 23	Individuals	Privacy	Nevada	1	—
Apr 21	Data Broker (Settlement)	Privacy	Alabama	1	—
Apr 21	Video Game Provider	Privacy	Alabama	1	—
Apr 10	AI Company	AI	Delaware	1	—
Mar 31	Social Media Company	Privacy	Connecticut	4	—
Mar 31	Communications Company	Cyber	Connecticut	2	$515,000
Mar 23	Genetic Testing Company	Privacy	South Dakota	1	—
Mar 12	Two Juveniles	Privacy	Pennsylvania	1	—
Mar 3	Sports Streaming Platform	Privacy	California	1	—
Feb 27	Automotive Manufacturer	Privacy	California	1	—
Feb 27	AI Company	AI	Pennsylvania	1	—
Feb 26	Consumer Electronics Manufacturer	Privacy	Texas	1	—
Feb 20	Online Retailer (Fast Fashion)	Privacy	Texas	1	—
Feb 19	Consumer Electronics Manufacturer	Cyber	West Virginia	1	—
Feb 19	IoT / Security Camera Manufacturer	Cyber	Texas	1	—
Feb 18	Drone Manufacturer	Privacy	Texas	1	—
Feb 17	Network Equipment Manufacturer	Cyber	Texas	1	—
Feb 17	Social Media Companies	Privacy	Oklahoma	1	—
Feb 11	Media & Entertainment Company	Privacy	California	1	—
Feb 4	Industry Trade Association	Privacy	Tennessee	1	—

INVESTIGATIONS AND ACTIONS (27) (CONT.)

Generic entity descriptions for regulatory investigations, enforcement actions, consent orders, and lawsuits against business defendants.

DATE	ENTITY TYPE	CATEGORY	LEAD STATE	STATES	SETTLEMENT
Feb 2	Pharmaceutical Companies	**Privacy**	Connecticut	1	—
Jan 14	AI Company	**AI**	California	36	—
Jan 8	AI Company (Chatbot Provider)	**AI**	Kentucky	57	—
Jan 8	Grocery Delivery Platform	**Privacy**	New York	1	—
Jan 8	Data Broker	**Privacy**	California	1	$45,000
Jan 1	Industry Trade Association	**Privacy**	Virginia	1	—

STATED REGULATOR ENFORCEMENT PRIORITIES (12)

Published guidance, advisories, AG coalition letters, and enforcement framework announcements.

DATE	JURISDICTION / DESCRIPTION	CATEGORY	LEAD STATE
Apr 16	Alabama — Privacy enforcement priorities	**Privacy**	Alabama
Apr 2	Oregon — AI governance / risk management guidance	**AI**	Oregon
Mar 31	42-State AG Coalition — Letter to Congress backing social media warning labels / AI chatbot safety	**AI**	Connecticut
Mar 24	New Mexico — AI governance priorities (government / law enforcement AI)	**AI**	New Mexico
Mar 17	Pennsylvania — Consumer-facing AI chatbot safety guidance	**AI**	Pennsylvania
Mar 16	Ohio — Privacy enforcement priorities (notice/transparency, data governance)	**Privacy**	Ohio
Mar 12	Pennsylvania — AI transparency / synthetic media enforcement framework	**AI**	Pennsylvania
Feb 27	Pennsylvania — AI governance / deceptive AI practices enforcement priorities	**AI**	Pennsylvania
Feb 26	Oklahoma — AG statement on DOJ request for voter data (financial/identity data)	**Privacy**	Oklahoma
Feb 19	Pennsylvania — Email marketing / CAN-SPAM enforcement guidance	**Privacy**	Pennsylvania
Jan 15	New Mexico — AI industry guidance (governance, synthetic media, fraud)	**AI**	New Mexico
Jan 13	Arkansas — AI governance / risk management priorities	**AI**	Arkansas

REGULATOR SWEEPS (4)

Coordinated, industry-wide enforcement campaigns.

DATE	TARGET / DESCRIPTION	CATEGORY	LEAD STATE
Mar 2	South Carolina — Unnamed privacy investigations **(2 actions)**	**Privacy**	South Carolina
Jan 13	New York — Data broker industry sweep	**Privacy**	New York
Jan 1	Oregon — Global Privacy Control compliance sweep	**Privacy**	Oregon

**Action counts in this report (307) exclude 7 pre-2020 actions and 37 North Carolina robocall actions filed on August 7, 2025 as part of a single, coordinated VoIP provider sweep. These Communications Privacy actions, while valid enforcement activity, would disproportionately skew state ranking and trend data. Including these actions, the total dataset contains 351 enforcement actions. Settlement figures also exclude the pre-2020 actions; all North Carolina robocall actions carried $0 settlements.*