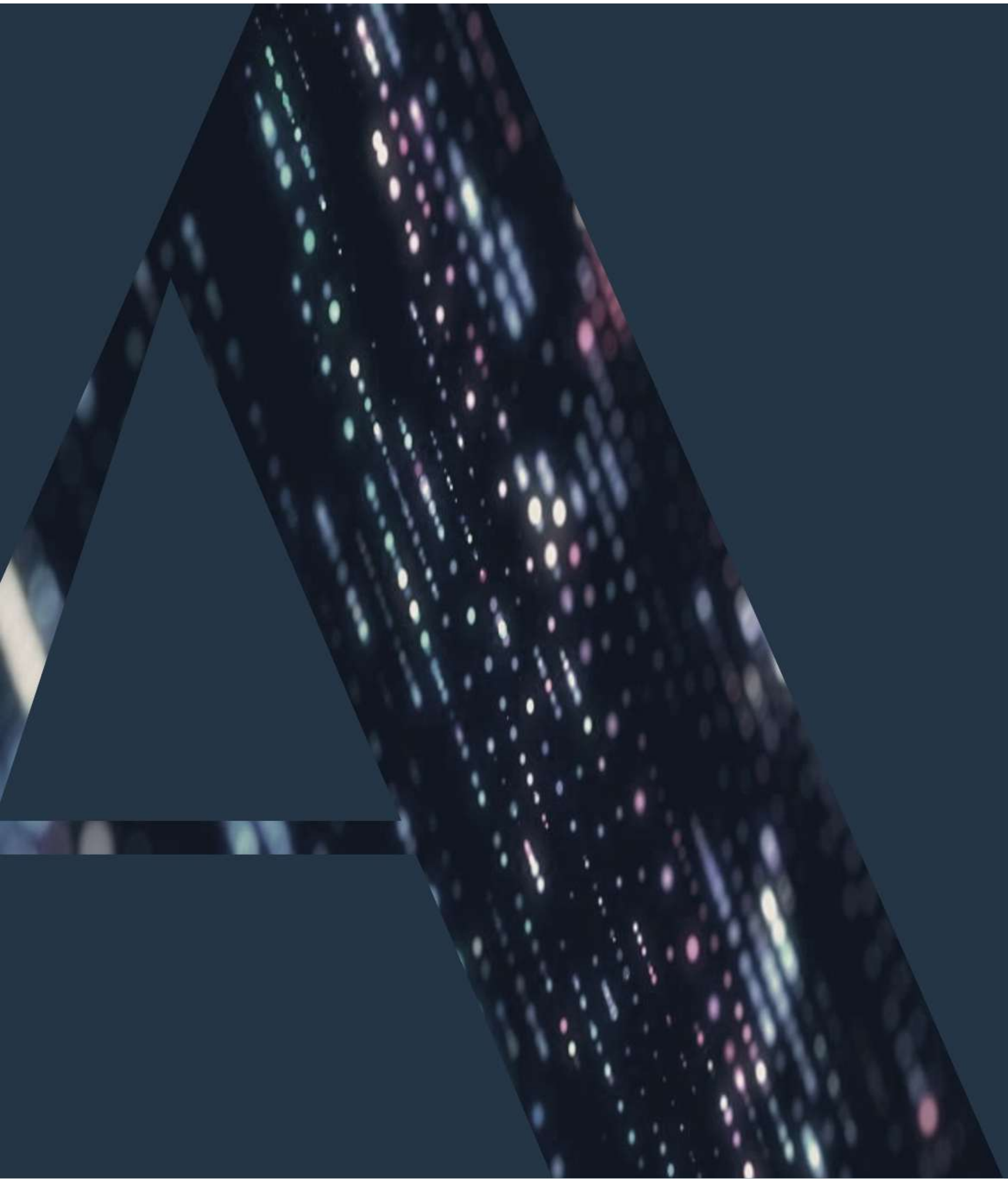


Association of Corporate Counsel, National Capital Region

# The Latest Updates in Privacy + Cybersecurity

February 10, 2026

**Evan Wolff**
Partner

Akin

**Rita Heimes**
Senior Counsel

Akin

*Moderated by:*

**Tony Pierce**
Partner

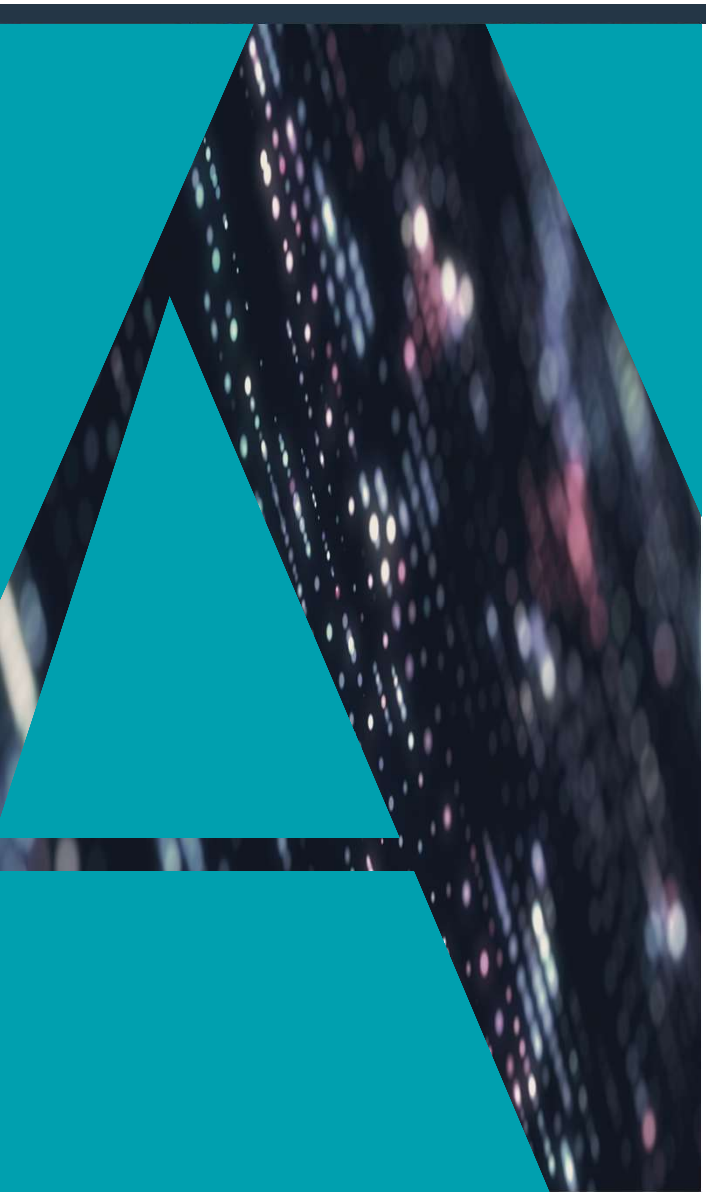
Akin

**Erica Bomsey**
Senior Vice President and
Deputy General Counsel

Leidos

**Note: panelists are each speaking in their individual capacity and not on behalf of their organizations.**

Akin℠



# Agenda

- Trends in Incident Response & Cyber Regulation
- Updates in Privacy & Data Protection
- Trends in Litigation and Enforcement for Security/Privacy
- Emerging AI Best Practices (and mistakes)
- Takeaways

# Trends in Incident Response & Cyber Regulation

# Cybersecurity Threats - What We’re Seeing (intro)

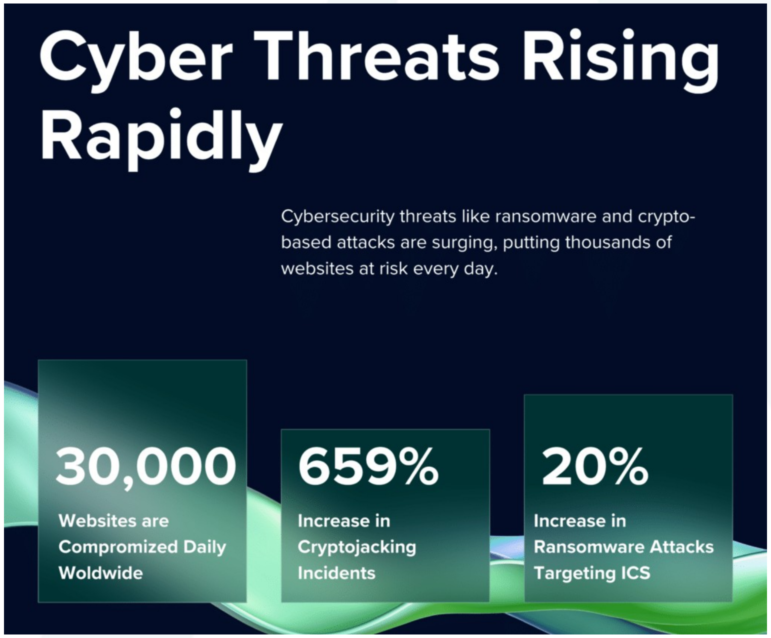
- Today’s cyber risk is driven by a diverse set of threat actors, ranging from financially motivated ransomware groups to nation-state-aligned espionage operators.
- These actors use distinct tactics, objectives, and targets, including ransomware, extortion, credential theft, espionage, and infrastructure disruption.
- The trends we will discuss reflect how attacks are evolving, not just what tools are used—focusing on identity abuse, cloud and collaboration platforms, and operational disruption.
- Essential to know: who is attacking, how they operate, and what they prioritize.

*“The 2025 threat environment is defined by speed, stealth, and ingenuity, with identity compromise, social engineering, and GenAI at the forefront.”*

**- Global Threat Report.**

*“From malware development to social engineering, adversaries are weaponizing AI to accelerate every stage of attacks, collapsing the defender's window of response.”*

**- Elia Zaitsev, CrowdStrike CTO.**



## Cyber Threats Rising Rapidly

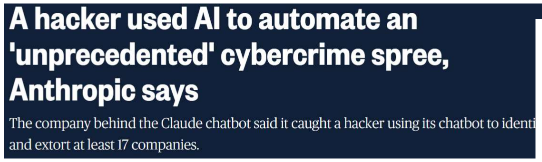
Cybersecurity threats like ransomware and crypto-based attacks are surging, putting thousands of websites at risk every day.

**30,000**
Websites are Compromized Daily Woldwide

**659%**
Increase in Cryptojacking Incidents

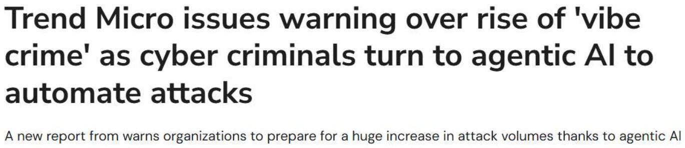
**20%**
Increase in Ransomware Attacks Targeting ICS

# AI-Driven Cybercrime



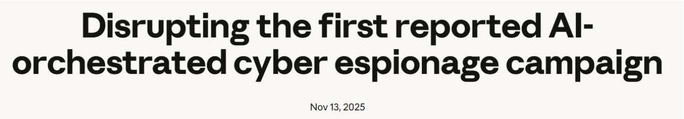
A hacker used AI to automate an 'unprecedented' cybercrime spree, Anthropic says

The company behind the Claude chatbot said it caught a hacker using its chatbot to identi and extort at least 17 companies.



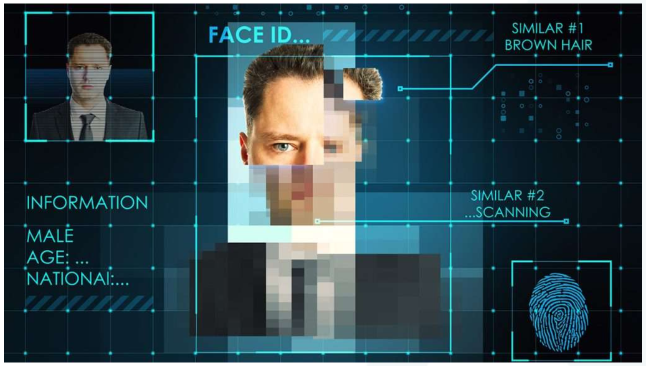
Trend Micro issues warning over rise of 'vibe crime' as cyber criminals turn to agentic AI to automate attacks

A new report from warns organizations to prepare for a huge increase in attack volumes thanks to agentic AI



Disrupting the first reported AI-orchestrated cyber espionage campaign

Nov 13, 2025



- **GenAI is accelerating social-engineering attacks** - criminals using AI-generated voices, video, and language models to impersonate executives and trusted employees (2024 Hong Kong deepfake fraud, where attackers used an AI-generated video of a CFO to steal over $25 million in a single wire transfer scheme).
- **AI-enhanced phishing and vishing operations** - produce highly personalized messages across email, SMS, and collaboration platforms, boosting credential theft and business email compromise.
- **Criminal use of “dark” AI models (e.g., WormGPT-style tools)** - lower barriers to writing malware, crafting ransomware notes, and automating reconnaissance, allowing less-skilled actors to execute sophisticated attacks.
- **Deepfake tech** - used to bypass controls, including synthetic voice attacks to defeat call-back procedures and video deepfakes used to manipulate help desks, vendors, and financial approval workflows.
- **AI-assisted fraud expanding** - affecting customer support, HR, and legal functions through fake job applicants, synthetic IT workers, and automated insider reconnaissance.

*AI does not create new crimes, it industrializes existing ones*

# Supply Chain Vulnerability: Expanding Attack Surface

> The CrowdStrike outage "reveals how a single point of failure in the complex web of supply chain services can trigger far-reaching consequences." — **Ken Huang**, cloud security expert for the Cloud Security Alliance (CSA).

- **Software and service providers remain high**-value entry points. SolarWinds, MOVEit, and 3CX – a compromise cascaded across thousands of downstream customers.
- **Managed service providers (MSPs) and cloud vendors are prime targets**. Attackers gain privileged access, broad visibility, and the ability to scale impact quickly across multiple organizations and sectors.
- **Identity and access in the supply chain is the weakest link**. Attackers use vendor credentials, remote access tools, and help-desk workflows rather than exploiting software flaws.
- **Open-source dependencies can introduce hidden risk**. Widely used libraries and updates provide opportunities for malicious code insertion or compromise upstream of enterprise controls.
- **Good strategic target for nation-state and criminal actors** – enabling espionage, long-term persistence, infrastructure disruption without directly attacking the ultimate target.
- **Supply-chain risk is not a third-party issue**, but a core enterprise risk requiring continuous monitoring, contractual controls, and incident-response integration.

# Cybersecurity Threat Landscape (2025 Highlights)

- Attackers relying less on pure data encryption and more on multi-stage campaigns designed to maximize operational pressure and decision-making speed.
- Double extortion expanded into infrastructure disruption, as threat actors increasingly combine data theft with intentional system outages, service degradation, and operational shutdowns.
- Critical infrastructure and professional services firms remain high-value targets, given the cascading impact of downtime across customers, regulated environments, and third-party ecosystems.
- Groups such as Scattered Spider have grown more sophisticated and more pernicious, using social engineering and identity-based access to compromise telecommunications providers and managed service environments at scale.
- The most disruptive incidents increasingly prioritize disabling infrastructure over stealing data, with nation-state patterns remaining distinct – Russia focused on disruption and destabilization; China on persistent data access and long-term intelligence collection.
- The cybersecurity marketplace in 2025 – reflects this threat shift. Organizations consolidating tools, demanding faster incident-response capabilities, and favoring vendors that integrate identity security, cloud visibility, and recovery over standalone point solutions.

# Recent Cybersecurity Threat Examples

- Scattered Spider –identity-centric intrusion, vishing, MFA fatigue, and abuse of remote access and collaboration platforms to compromise telecommunications, technology, and professional services firms (often precursor to ransomware or extortion).
- **Ransomware-as-a-service affiliates (e.g., Qilin / REVENANT SPIDER)** still effectively exploiting compromised remote administration tools, moving laterally with built-in system utilities, and encrypting or exfiltrating financially critical data to accelerate payment pressure.
- **Social-engineering-driven eCrime groups** (e.g., SCATTERED SPIDER) – leveraging trusted enterprise platforms like Microsoft Teams for vishing and malware delivery, bypassing traditional email-centric security controls and targeting credentials rather than exploits.
- **Financially motivated data-theft crews tied to brands like ShinyHunters** – increased tempo of extortion-only campaigns, focusing on rapid exfiltration, cryptocurrency theft, and reputational leverage rather than prolonged dwell time or encryption.
- **China-aligned state actors (e.g., WARP PANDA)** – target U.S. technology and manufacturing sectors, deploying sophisticated implants to achieve persistent access and intellectual-property theft, reinforcing a long-term data-collection strategy rather than immediate disruption.
- Common thread – shift toward identity abuse, trusted-tool exploitation, and operational impact, where the goal is increasingly access and disruption, not just malware execution.

# Insider Threats (Malicious & Accidental)

- Bribery for access: employees have been offered money to exfiltrate data and/or plant malware.
- Buying credentials/recruiting insiders: **LAPSUS$ playbook**. the group paid employees or contractors at target firms (or their suppliers) to obtain credentials or persuade help desks to reset MFA, a pattern echoed across the 2022 Okta/Sitel episode.
- Nation-state exploitation of insiders. An ex-manager was convicted for taking gifts and cash from foreign government officials to **access private data on dissidents**.
- Nation-state economic espionage via insider access (PRC). **Engineers have committed economic espionage to benefit China-based ventures**—highlighting how privileged insiders can move crown-jewel IP at scale.
- **Telecom/tech exposure through social-engineering of insiders (Scattered Spider)**. The group has repeatedly impersonated employees and pressured help desks to reset MFA or credentials, enabling access at large telcos, retailers, airlines, and casinos, illustrating how "help desk as front door" turns staff into unwitting insiders.
- Accidental insider: AI-enabled data spill. Engineers at multinationals have **pasted confidential source code and meeting notes into ChatGPT**, unintentionally exposing trade secrets and prompting new internal AI controls—an example of LLM-driven data exfiltration without malware.

# APTs & Nation-State Cyber Activity

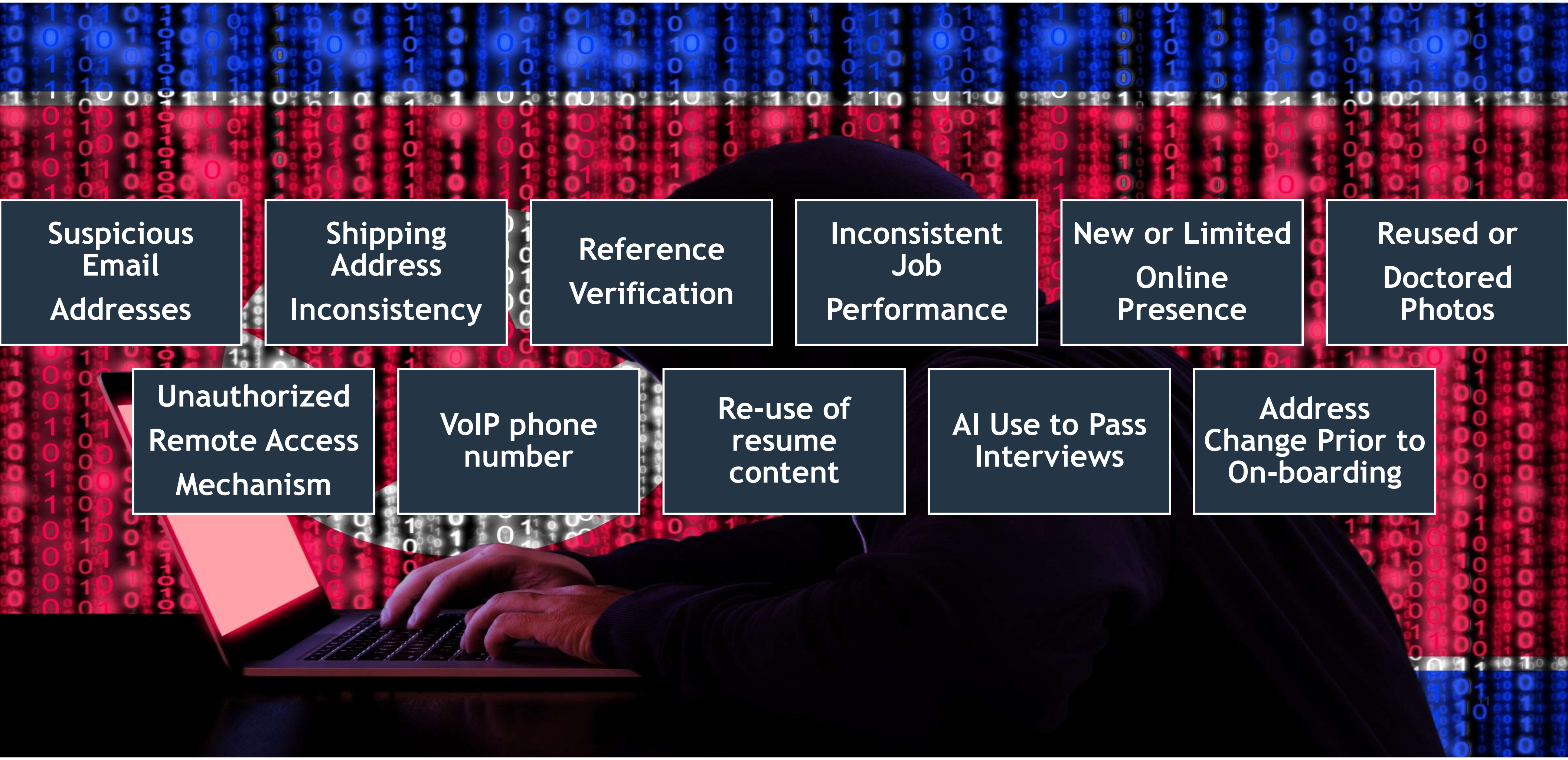
- **China-aligned "Typhoon" actors (Volt, Flax, Salt Typhoon)** continue to evolve toward pre-positioning and persistence, embedding themselves in networks tied to telecommunications, energy, and transportation rather than pursuing immediate disruption.

- **Russia-aligned operations remain focused on disruption**, using cyber activity to degrade or threaten energy, utilities, and public-facing infrastructure, particularly during periods of geopolitical tension.

- **North Korean actors increasingly rely on "fake IT worker" operations**, placing operatives into U.S. and allied companies to gain trusted access, generate revenue for the regime, and facilitate espionage or theft.

- Advanced persistent threats remain one of the most consequential cyber risks in 2026, as nation-state actors conduct long-running, stealthy intrusions designed to maintain durable access to targeted networks for espionage, influence, and potential disruption rather than immediate financial gain.
- U.S. intelligence and cybersecurity agencies consistently identify China, Russia, Iran, and North Korea as the most active state sponsors of APT operations, each pursuing distinct strategic objectives ranging from intelligence collection and intellectual-property theft to political influence and critical-infrastructure reconnaissance.

# Red Flags - Spotting North Korean Candidates



- Suspicious Email Addresses
- Shipping Address Inconsistency
- Reference Verification
- Inconsistent Job Performance
- New or Limited Online Presence
- Reused or Doctored Photos
- Unauthorized Remote Access Mechanism
- VoIP phone number
- Re-use of resume content
- AI Use to Pass Interviews
- Address Change Prior to On-boarding

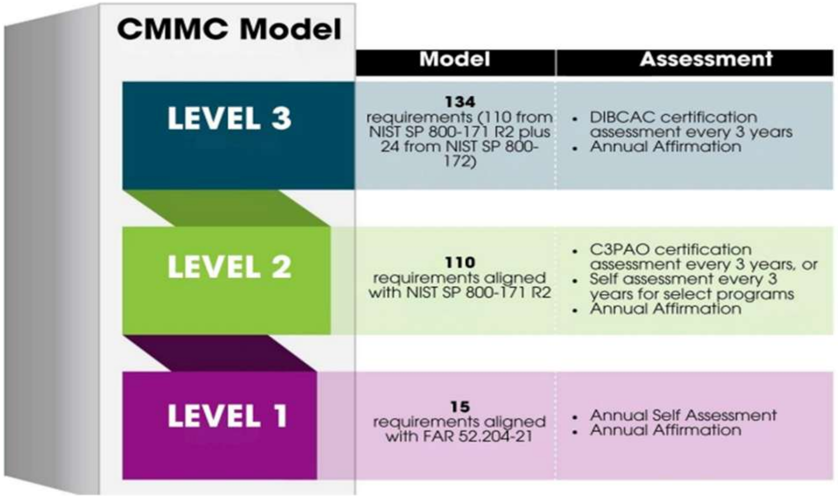
# Digital Forensics Trends & Complex Investigations

- Digital forensics is increasingly driven by incident-readiness planning, as organizations recognize that speed, defensibility, and completeness depend on advance preparation rather than ad-hoc response.
- Incident response and forensics providers have rapidly become cloud-native, building expertise in platforms such as Microsoft 365, Google Workspace, AWS, and Azure, and relying on API-based collection rather than physical imaging.
- AI-enabled analytics are increasingly used by forensic teams to triage massive data volumes, identify anomalous activity, correlate logs across environments, and accelerate early-stage scoping without substituting for human judgment.
- **Lawyer**: central coordinating role, shaping investigative scope, preserving privilege, managing regulators, and aligning forensic work with disclosure and litigation strategy.
- **Forensic vendors**: technical translators, converting highly complex findings into timelines and narratives that can withstand regulatory, board, and adversarial scrutiny.
- **PR & Comms**: external messaging decisions increasingly intersect with regulatory timelines, customer trust, and litigation exposure.

# Incident Reporting Regulatory Changes

- **Public companies continue to adjust to the SEC's cybersecurity incident disclosure regime, which requires reporting material cybersecurity incidents within four business days after a materiality determination.**
- FTC's amended Safeguards Rule, effective May 13, 2024, now requires non-banking financial institutions subject to FTC jurisdiction to notify the FTC within 30 days of discovering a security incident involving unencrypted customer information of 500 or more consumers, significantly expanding federal breach-reporting obligations.

- **DFARS 252.204-7012** – requires reporting covered cyber incidents to the DoD within 72 hours of discovery, safeguarding Controlled Unclassified Information (CUI), and flowing reporting obligations down the supply chain; these reporting duties operate in parallel with the phased rollout of **CMMC certification requirements** beginning in late 2025.
- In EU: **NIS2** expands the scope of entities subject to cybersecurity incident reporting and imposes tight, multi-stage notification timelines (early warning, incident notification, and final report). Implementation varies across Member States.



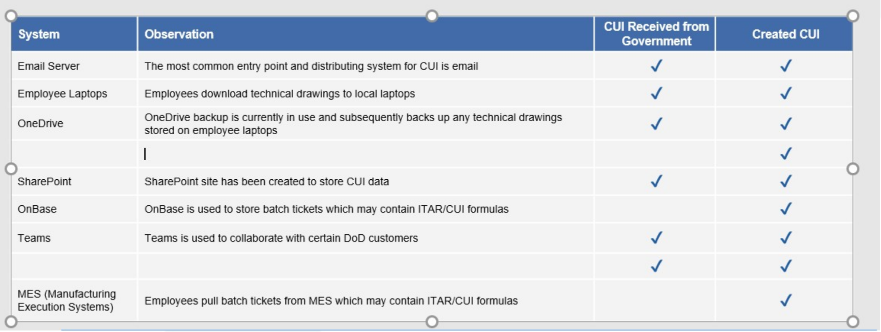
**CMMC Model**

| | Model | Assessment |
|---|---|---|
| LEVEL 3 | **134** requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172) | • DIBCAC certification assessment every 3 years<br>• Annual Affirmation |
| LEVEL 2 | **110** requirements aligned with NIST SP 800-171 R2 | • C3PAO certification assessment every 3 years, or<br>• Self assessment every 3 years for select programs<br>• Annual Affirmation |
| LEVEL 1 | **15** requirements aligned with FAR 52.204-21 | • Annual Self Assessment<br>• Annual Affirmation |

# Cybersecurity Maturity Model (CMMC) Final Rule

- DoD’s CMMC DFARS rule was finalized on September 10, 2025 and became effective November 10, 2025, launching a three-year phased rollout with Levels 1–3 tied to FCI/CUI sensitivity.
- Three certification levels:
  - **Level 1**: Basic safeguards for FCI
  - **Level 2**: NIST SP 800-171 compliance for CUI
  - **Level 3**: Enhanced controls aligned with NIST SP 800-172 for critical programs
- Final DFARS rule effective: November 10, 2025, making CMMC a mandatory contract requirement, not guidance

- Phased rollout (2025–2028):
  - Year 1: Level 1 & 2 self-assessments
  - Year 2: Third-party Level 2 certifications
  - Year 3: Level 3 certifications
  - Year 4: Universal enforcement across covered contracts
- Continuous compliance: Annual affirmations and current status required in SPRS for awards, renewals, and option exercises



| System | Observation | CUI Received from Government | Created CUI |
|---|---|---|---|
| Email Server | The most common entry point and distributing system for CUI is email | ✓ | ✓ |
| Employee Laptops | Employees download technical drawings to local laptops | ✓ | ✓ |
| OneDrive | OneDrive backup is currently in use and subsequently backs up any technical drawings stored on employee laptops | ✓ | ✓ |
| | | | ✓ |
| SharePoint | SharePoint site has been created to store CUI data | ✓ | ✓ |
| OnBase | OnBase is used to store batch tickets which may contain ITAR/CUI formulas | | ✓ |
| Teams | Teams is used to collaborate with certain DoD customers | ✓ | ✓ |
| | | ✓ | ✓ |
| MES (Manufacturing Execution Systems) | Employees pull batch tickets from MES which may contain ITAR/CUI formulas | | ✓ |

# State and Sector-Specific Cybersecurity Rules

## State-Level Cybersecurity Requirements

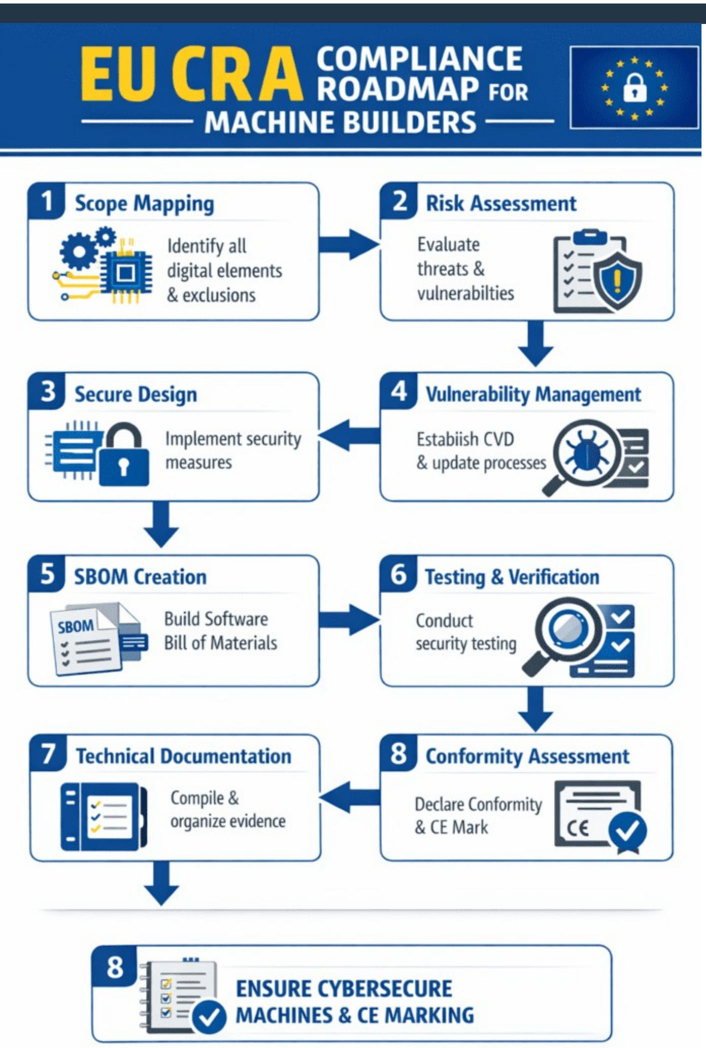
- Operational security mandates: States increasingly impose affirmative cybersecurity obligations, not just breach notification (e.g., reasonable safeguards, risk assessments, audits).
- Sector-targeted rules: Financial services, healthcare, utilities, education, and data brokers face heightened, prescriptive controls.
- Enforcement-first approach: State AGs and regulators are using consumer protection and privacy laws to enforce cybersecurity failures, even without sector-specific statutes.
- Cyber tied to privacy compliance: Security failures are treated as privacy violations, expanding penalty exposure.

## Key Sector-Specific Regimes

- State rules modeled on NYDFS-style cybersecurity programs: governance, testing, incident reporting, and vendor risk management.
- Healthcare: Expanded expectations beyond HIPAA, including ransomware preparedness, third-party oversight, and system resilience.
- Critical Infrastructure & Utilities: State-level alignment with federal resilience and incident-reporting expectations.
- Data Brokers & Ad Tech: Cybersecurity obligations tied to registration, audits, and data-minimization duties.

## Cross-Cutting Trends

- From “reasonable security” to defined controls: Regulators expect documented programs, not ad hoc practices.
- Vendor and supply-chain focus: Security obligations increasingly extend to service providers and downstream partners.
- Incident readiness as a compliance requirement: Testing, tabletop exercises, and post-incident remediation are scrutinized.


EU CRA COMPLIANCE ROADMAP FOR MACHINE BUILDERS
1 Scope Mapping
Identify all digital elements & exclusions
2 Risk Assessment
Evaluate threats & vulnerabilties
3 Secure Design
Implement security measures
4 Vulnerability Management
Estabiish CVD & update processes
5 SBOM Creation
SBOM
Build Software Bill of Materials
6 Testing & Verification
Conduct security testing
7 Technical Documentation
Compile & organize evidence
8 Conformity Assessment
Declare Conformity & CE Mark
CE
8
ENSURE CYBERSECURE MACHINES & CE MARKING

# EU Cyber Resilience Act (CRA): Key Highlights

1. The EU Cyber Resilience Act is one of the most sweeping product-security laws globally, applying to most hardware and software with digital elements placed on the EU market, regardless of where the manufacturer is based.
2. CRA mandates **“secure-by-design and secure-by-default” requirements**, imposing affirmative cybersecurity obligations throughout a product’s entire lifecycle, from design and development through post-market support.
3. Products are subject to ongoing vulnerability handling and patching duties, including **mandatory vulnerability and incident reporting**, with reporting obligations beginning in September 2026.
4. framework introduces **risk-based product categories**, with heightened compliance, documentation, and conformity assessment requirements for “important” and “critical” products, significantly increasing operational and compliance burdens for certain companies.
5. Enforcement risk is material, with potential **significant administrative fines, market withdrawal, and restrictions on EU market access for non-compliant products**.
6. CRA follows a **phased implementation timeline**, with core obligations beginning in June 2026 and full application by December 2027, making early product, vendor, and governance alignment essential for continued EU market access.

# Updates in Privacy & Data Protection: US, EU and Beyond

# U.S. State Privacy Law Updates

**No new comprehensive state privacy laws, but... several amendments!**

- First there was the EU GDPR
- Then, there was the CCPA as amended by the CPRA
- Now, 20 states have comprehensive consumer privacy laws
- 2025 was the first year since 2020 that did not add any new laws
- But state AGs are working with legislatures to amend laws to close loopholes, respond to technological advances

  Connecticut, Montana, Oregon, Colorado

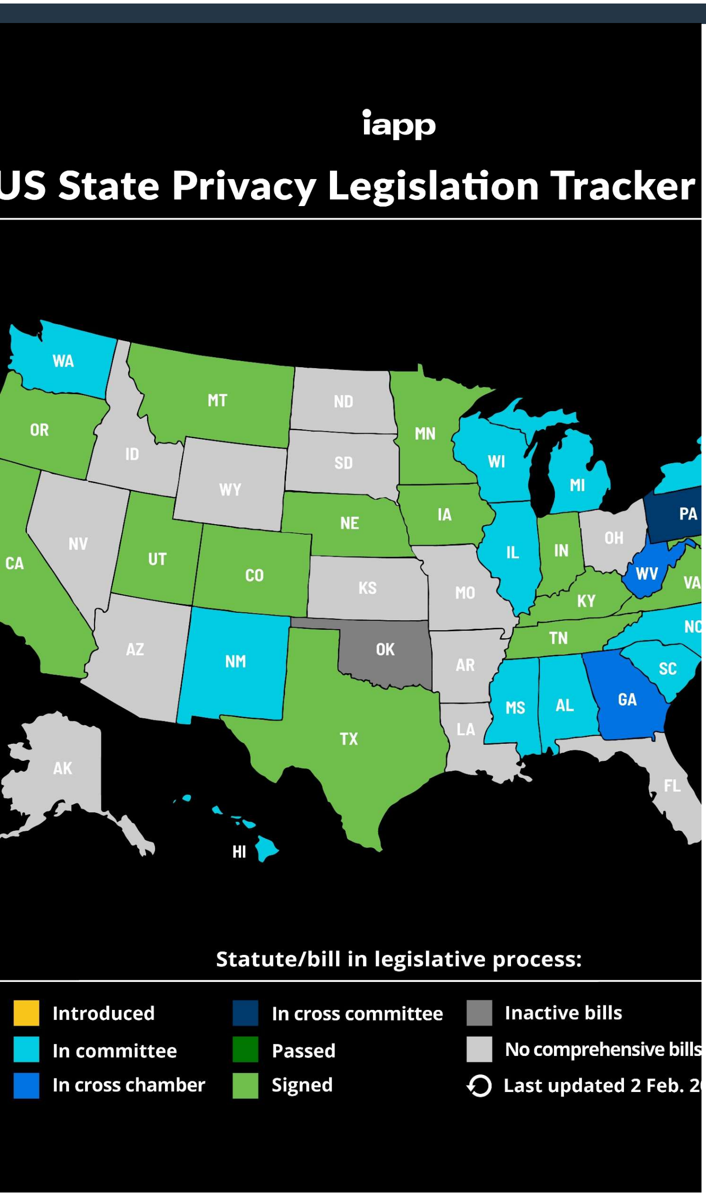
  Texas, Virginia, California

## CCPA Rulemaking

- New CCPA regulations finalized: CPPA finalized major CCPA updates covering automated decision-making technology (ADMT), risk assessments, and cybersecurity audits, with regulations effective January 1, 2026 and phased-in compliance timelines.

## Colorado & New Jersey Rulemaking

- Expansion, clarification of enforcement expectations, and more prescriptive requirements. Focus on universal opt-out mechanisms, biometric data, and profiling/automated decision-making.



# U.S. State Privacy Law Updates

## Age-Appropriate Design Code Laws - 2025

Arkansas, California, Louisiana, Montana, Nebraska, Texas, Utah and Vermont

South Carolina, passed February 5, 2026 - personal liability for officers and employees

- Age Assurance
- First Amendment

## Data Brokers: states imposing obligations on businesses that collect & sell personal data without a direct consumer relationship

## California - DELETE Act

DELETE Act: The California Privacy Protection Agency (CalPrivacy) enforcement actions against data brokers for failure to register and comply with Delete Act requirements. Penalties accruing per day for non-registration.

- Centralized deletion mechanism (DROP): CalPrivacy is implementing the Delete Request and Opt-Out Platform, enabling consumers to submit a single deletion request to all registered data brokers.

**Texas**: Expands coverage to any entity transferring data it didn't directly collect

# U.S. State Privacy Law Updates

## Enforcement Activity

- California AG and CalPrivacy continue aggressive enforcement focused on opt-out mechanics, targeted advertising, children’s data, and sensitive data.
- Bipartisan coalition of privacy regulators formed (2025): Attorneys general from multiple states, with the CalPrivacy, established a privacy enforcement consortium to coordinate investigations, share intelligence, and pursue multistate cases.
- Texas Data Privacy and Security Act (TDPSA) took effect (July 1, 2024), the Texas AG has brought high-profile cases involving geolocation data, data brokers, sensitive data, and children’s privacy. Aggressive use of state consumer protection authority.

## In summary

- **Kids and Teens** – major enforcement priority for State AGs.
- **Regulators are checking out your website**

>cookie consent policies

>privacy policies must accurately reflect customers’ rights in their state

>when was policy last updated

# U.S. Federal Law Updates

## Still no federal comprehensive privacy law - but 18 children’s online safety bills advanced to full committee

## Federal Trade Commission (FTC) Enforcement Priorities

- **KIDS:** COPPA Rule finalized (Jan. 16, 2025) — Amended Children’s Online Privacy Protection Rule adds opt-in for third-party ads, tighter retention/data-minimization, and clarifies mixed-audience coverage; effective June 23, 2025.
- **DATA TRANSFERS**: FTC **has enforcement authority over Protection Americans Data from Foreign Adversaries Act (PADFAA)**
  - **Applies to data broker**s; prohibits transfer to any entity owned directly **or indirectly by entities in country of concern; broad definition of sensitive data**

## Department of Justice: Bulk Data Rule Restricts Sensitive Data Transfers

### Enforced by DOJ — Data Security Program (DSP)

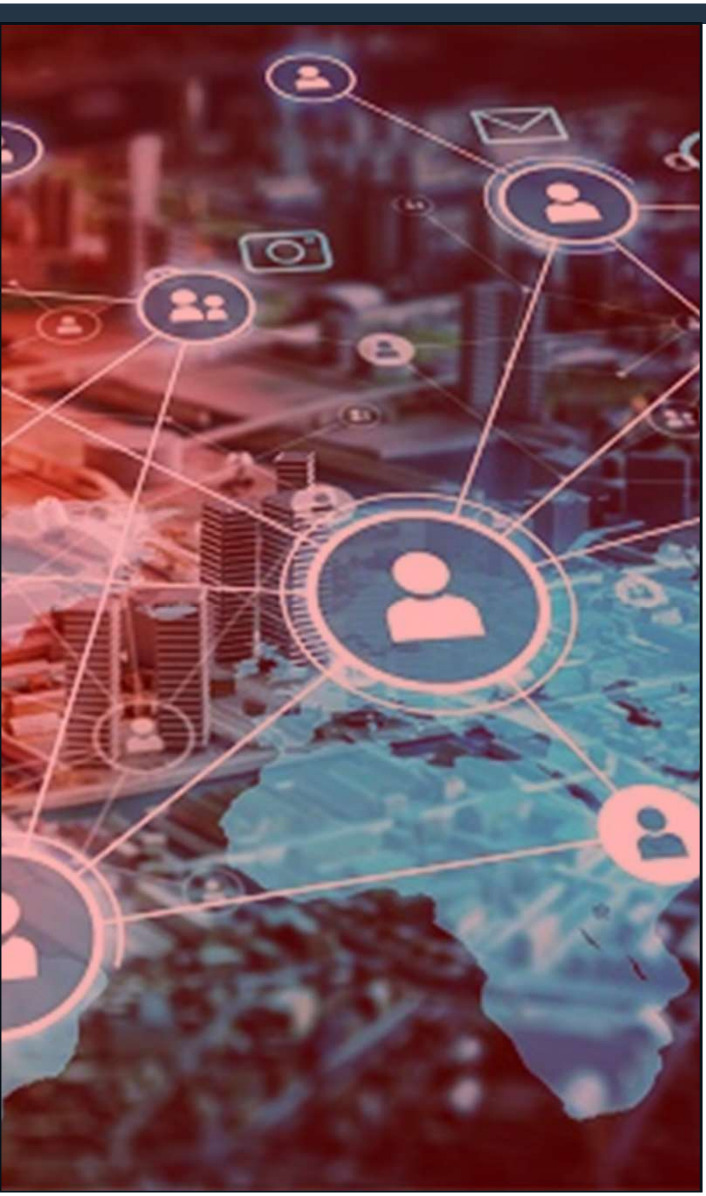
- DOJ Final Rule implementing EO 14117 (Jan. 8, 2025; effective Apr. 8, 2025) — Establishes 28 C.F.R. Part 202 to prohibit/restrict certain transactions involving bulk U.S. sensitive personal data and U.S. government-related data with countries of concern; enumerates covered categories

### Enforced by FTC — PADFAA

- PADFAA enacted (Apr. 24, 2024) — Protecting Americans’ Data from Foreign Adversaries Act of 2024 (Pub. L. 118-50, Division I) bars data brokers from transferring U.S. individuals’ sensitive data to foreign adversaries

# Cross-Border Laws: DOJ “Bulk Data Rule” / (DSP)

- The DOJ’s Data Security Program, effective in 2025, creates a national-security-driven control regime over “bulk” U.S. sensitive personal data and U.S. government-related data, including precise geolocation, biometric identifiers, human genomic and other ’omic data, personal health data, personal financial data, and certain personal identifiers once specified volume thresholds are met.
- Prohibited transactions: such as certain data-brokerage and human ’omic data transfers to countries of concern. Restricted transactions: may proceed only if stringent privacy, cybersecurity, governance, and access-control requirements are satisfied.
- For restricted transactions – CISA issued mandatory security requirements (organizational governance controls, identity and access management, logging and monitoring, data-level protections, and auditable compliance processes).
- The DSP applies across vendor, employment, investment, and data-broker relationships, operates independently of privacy concepts like de-identification or encryption, and effectively functions as an export-control-style regime for data.
- Enforcement expectations – DOJ signaling active oversight following initial guidance and grace periods, and violations carrying potential civil penalties and criminal exposure, making early “know-your-data” inventories and transaction mapping critical for 2026 risk management.



# Cross-Border Laws: PADFAA

Data Transfer Restrictions

- Bright-line prohibition: unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available a U.S. individual's personally identifiable sensitive data to a foreign adversary country or any entity controlled by a foreign adversary.
- Covered recipients: "Foreign adversary countries" are designated in federal law; PADFAA also captures entities "controlled by" such countries (e.g., ownership/control tests), closing common routing/affiliate gaps.
- Scope of "personally identifiable sensitive data": Includes government identifiers, financial account data, precise geolocation, health/genetic data, and other categories.

Impact on Data Brokers & Platforms (What Is a "Data Broker"?)

- Definition — "Data broker": A business that collects and sells or licenses Americans' personally identifiable sensitive data, without a direct relationship to the individual = falls within PADFAA's "data broker" scope (as defined in the Act).
- Immediate compliance consequences: Brokers must block transactions involving covered recipients; implement counter-party diligence and contractual controls to prevent onward transfers to foreign-controlled entities.
- Platforms & app ecosystems: Ad networks, SDK providers, and marketplaces that aggregate or broker access to sensitive datasets face exposure if they sell or provide access to covered recipients (even via resellers).

# EU Significant Developments

**European Commission’s Digital Omnibus Proposals:**

- introduced in November 2025
- aims to streamline the EU’s digital rulebook by amending several key laws, including the **GDPR.** Proposals include:
  - clarifying that pseudonymized data is not "personal data" if the controller cannot reasonably re-identify the individual, even if a third party could.
  - explicitly allowing the use of personal data for training AI models under "legitimate interests,“
  - updating and harmonizing cookie rules for first-party cookies and to mitigate consent fatigue;
  - extending data breach reporting to 96 hours

**Stay tuned!**

# Top 2025 Global Developments

**Australia:**

- New statutory tort for serious invasions of privacy, allowing privacy rights of action as of June 2025
- Social media age 16 minimum age requirements in force as of December 2025

## India: *Digital Personal Data Protection Act 2023*

- DPDP Rules now in effect as of November 2025
- Consent-based requirements
- Nove “Consent-manager” ecosystem

## China: *Personal Information Protection Law*

- Organizations handling “important” data subject to mandatory security assessments by Cyberspace Administration of China: Cyber + Privacy laws converging and unifying
- Localization requirements and restrictions on outbound transfers

# Litigation and Enforcement Trends in Security/Privacy

Justice Department Cyber Fraud Push Yields Wave of Settlements

Recent Cybersecurity FCA Settlement Demonstrates Heightened FCA Risk to Government Contractors

# Federal trends: (FCA, EO)

- Cyber & procurement theories: FCA use tied to cybersecurity representations, contract compliance, and grant/defense procurement.
- The DOJ recovered a record **$6.8B** in FCA settlements/judgments in FY 2025, and while healthcare dominated, cybersecurity related FCA resolutions continued under the Civil Cyber Fraud Initiative.
- Materiality: Evidence of government payment behavior is central; compliance deviations tied to payment conditions get priority.
- 2025 included notable cybersecurity FCA settlements reinforcing that false certifications of cyber compliance create material FCA risk for contractors and grantees.

# FTC: Kids + Teens, Deceptive AI

- **COPPA Rule**: Finalized in 2025

  >Violations for knowingly collecting data from children w/o appropriate parental notice and consent

- **Section 5 “deception” claims:**

  >certain business practices involving children and teens considered **deceptive** trade practices

  >maintaining sensitive data longer than reasonably expected

  >claims about **AI PRODUCT PERFORMANCE considered deceptive:**

  **-”guaranteed profits”**

  **-”accuracy”**

  **-”legally compliant outcomes”**

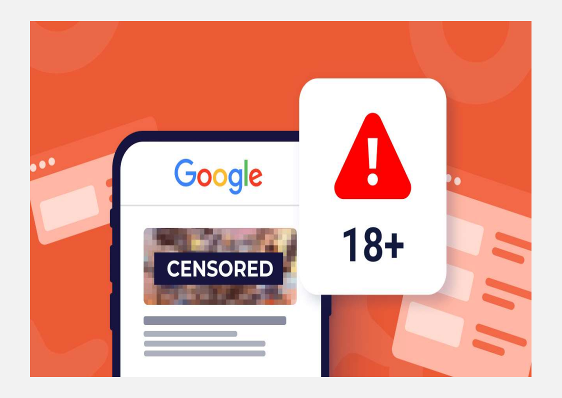
- **2026 Issues:**

  **>Age Verification Complexities**

  **>Consumer injuries and benefits in data-driven economy**

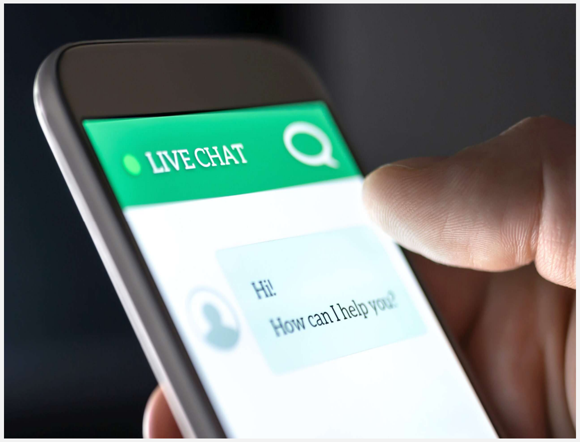
# State AG Privacy Enforcement: Actions & Focus

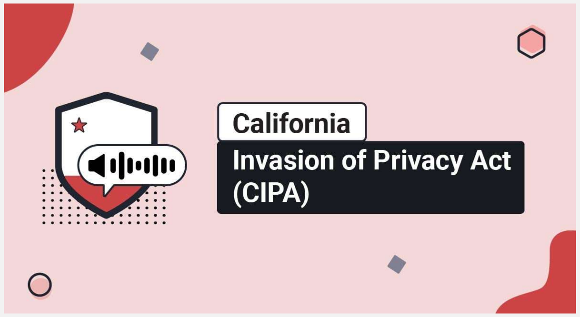
- 15 new enforcement actions announced, filed, or settled, with **Texas** and **California** leading the way.
- **Texas:** Lawsuits involving driver behavior data and smart products' collection of sensitive data
- **California:** Focused on cookie/tracker-related alleged violations; user experience, asymmetrical privacy controls; failure to provide consumers with effective opt-out / enforcement of the DELETE Act (failure to register as data broker)
- **Utah: -** Youth privacy and online safety
- **Florida: -** Processing and selling sensitive and children's data without consent
- **Connecticut:** Noncompliant privacy notice
- **Consortium of US Privacy Regulators:** coordinating investigations and sharing best practices



# Plaintiffs: Old Bottle, New Whine?

- **Wiretap Laws:**
  - —CIPA and ECPA:
    - Courts in 2025 limited some CIPA pen register theories and scrutinized Article III standing yet claims persisted under alternative wiretap and privacy statutes.
- **Video Privacy Protection:**
  - —VPPA exposure turns on whether site operators are "video tape service providers" and whether identifiers constitute PII linking users to specific video content.
- **Colorado's PFTA:**
  - —Will we see more class actions against companies possessing cell phone #s?





# Litigation Trends

- **Private Right of Action (PRA)** remains an enforcement driver, particularly under the CCPA and CPRA, with plaintiffs continuing to use breach-related security claims and parallel state statutes to supplement regulatory enforcement and accelerate litigation timelines.
- **Pixel, session-replay, and wiretapping litigation** continues to evolve: courts increasingly scrutinizing consent, standing, and "in-transit" interception theories, producing mixed results under CIPA, the federal Wiretap Act, and the VPPA rather than uniform plaintiff victories.
- **Biometric privacy claims** remain active, driven primarily by Illinois' BIPA, with courts refining damages exposure, standing, and what constitutes a single "violation," while biometric data continues to be treated as uniquely high-risk and difficult to remediate once compromised.
- **AI-related litigation** *(e.g. Bartz v. Anthropic)* expanded in 2025, including claims tied to biometric data use, training data practices, discrimination, and consumer deception, signaling that AI deployment increasingly creates privacy, civil-rights, and product-liability exposure alongside regulatory scrutiny.
- **Capital One litigation** – (*Willoughby v. Capital One Financial Corp.*)demonstrated how cloud misconfiguration and security failures can generate exposure across class actions, settlements, and regulatory scrutiny, shaping expectations for "reasonable security" and post-incident remediation.

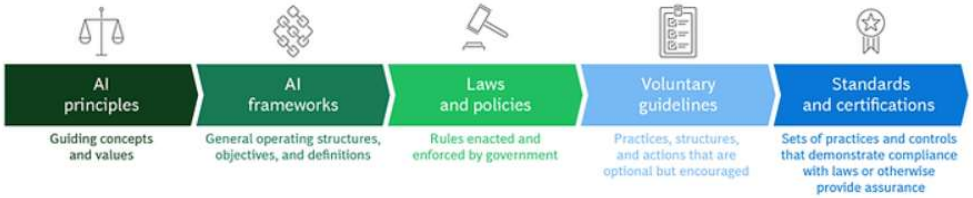
# Emerging AI Best Practices (and mistakes)

# AI trends (use in security, compliance, legal)

- Organizations using AI to accelerate threat detection, compliance monitoring, and legal workflows, but governance requirements under the EU AI Act and CalPrivacy ADMT rules are increasing documentation, testing, and human review obligations rather than reducing compliance workload.
- Companies piloting AI “corridors/sandboxes” to validate accuracy, safety, and privacy in controlled environments, aligning with AI Act’s emphasis on codes of practice and supervised experimentation.
- Threat actors are widely discussed as harvesting encrypted data now for future quantum decryption (“harvest now, decrypt later”): elevates the importance of crypto-agility and prudent minimization for long lived data.

# AI Governance in 2025

- Organizations are formalizing AI risk management programs, integrating AI use cases into existing enterprise risk, privacy, security, and compliance frameworks rather than treating AI as a standalone issue.
- Model documentation and transparency expectations have increased, with regulators and stakeholders focusing on inventories of AI systems, clear descriptions of purpose and data sources, and documentation sufficient to explain outcomes and support audits.
- Vendor and third-party AI assessments are now a core governance control, as organizations are held accountable for risks introduced by external models, embedded AI features, and downstream data use.
- Governance structures increasingly emphasize clear management ownership and escalation paths, ensuring defined responsibility for AI deployment decisions, monitoring, and corrective action.
- Crypto-agility and security planning are emerging considerations for AI systems, particularly where long-term data sensitivity, encrypted training data, and future cryptographic risks intersect with AI lifecycle management.



AI principles

Guiding concepts and values

AI frameworks

General operating structures, objectives, and definitions

Laws and policies

Rules enacted and enforced by government

Voluntary guidelines

Practices, structures, and actions that are optional but encouraged

Standards and certifications

Sets of practices and controls that demonstrate compliance with laws or otherwise provide assurance

# AI Regulatory Activity

## Federal

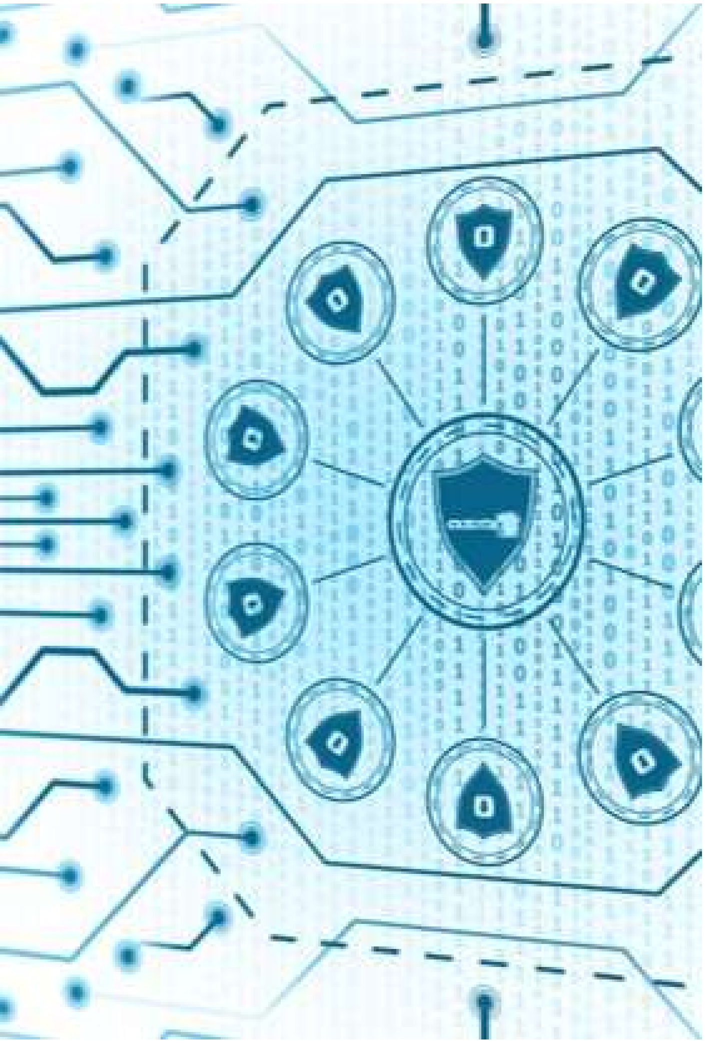
- No single federal AI statute, expansion of agency-led regulation and enforcement (FTC, SEC, DOJ, EEOC, CFPB, HHS).
- Rulemaking via existing authorities.
- NIST as the backbone: AI Risk Management Framework (AI RMF) and supporting guidance increasingly treated as a de facto compliance benchmark, including for government contractors and regulated industries.

## State

- Patchwork acceleration: states advancing AI-specific bills targeting automated decision-making, transparency, and consumer rights.
- Biometric expansion: broader definitions and enforcement under biometric, health, and children’s data laws (e.g., facial recognition).
- California as pace-setter: AI governance embedded in broader privacy, risk-assessment, and automated decision-making regimes.

## EU

- EU AI Act adopted (2024); implementation rolling through 2025–2026.
- Risk-based regime: bans on certain practices; strict obligations for high-risk AI systems; transparency duties for general-purpose and generative AI.
- High-risk sectors: healthcare, employment, credit, education, law enforcement.



# AI-Related Enforcement Actions

- FTC enforcement has focused on deceptive and unfair AI practices, including cases involving use of facial recognition beyond disclosed purposes, and cases involving allegedly biased facial-recognition deployment with inadequate safeguards.
- Employment and hiring algorithms remain a priority, illustrated by the EEOC's iTutorGroup settlement, where automated screening tools were found to unlawfully exclude older applicants, signaling continued scrutiny of AI-driven employment decisions.
- Biometric and facial-recognition enforcement continues, with actions and settlements involving Clearview AI and others reinforcing that consent, purpose limitation, and retention controls are mandatory ((not optional)) when AI processes biometric data.
- State and local regulators are moving from rulemaking to enforcement, including New York City's Local Law 144, which requires bias audits and notices for automated employment decision tools and is increasingly treated as an enforceable compliance obligation.
- GenAI practices are now under active regulatory review, with the FTC and state AGs examining claims around training data, consumer transparency, and misuse of personal data, even where no standalone "AI law" applies.
- Existing consumer protection, civil rights, and privacy laws are being actively applied to AI, eliminating any perceived enforcement gap while AI-specific regimes continue to mature.

# Common AI Compliance Failures

### Training Data Misuse

- Use of licensed, personal, or sensitive data without clear rights or documented purpose limitations.

- Over-collection and reuse of data beyond original disclosure or consent context.

- Weak vendor transparency around model training sources and downstream reuse.

### Hallucination & Output Risk

- Deployment of AI in decision-critical workflows without guardrails or human review.

- Inadequate controls to prevent fabricated facts, citations, or legal/medical conclusions.

- Reliance on AI outputs that contradict internal policies or public disclosures.

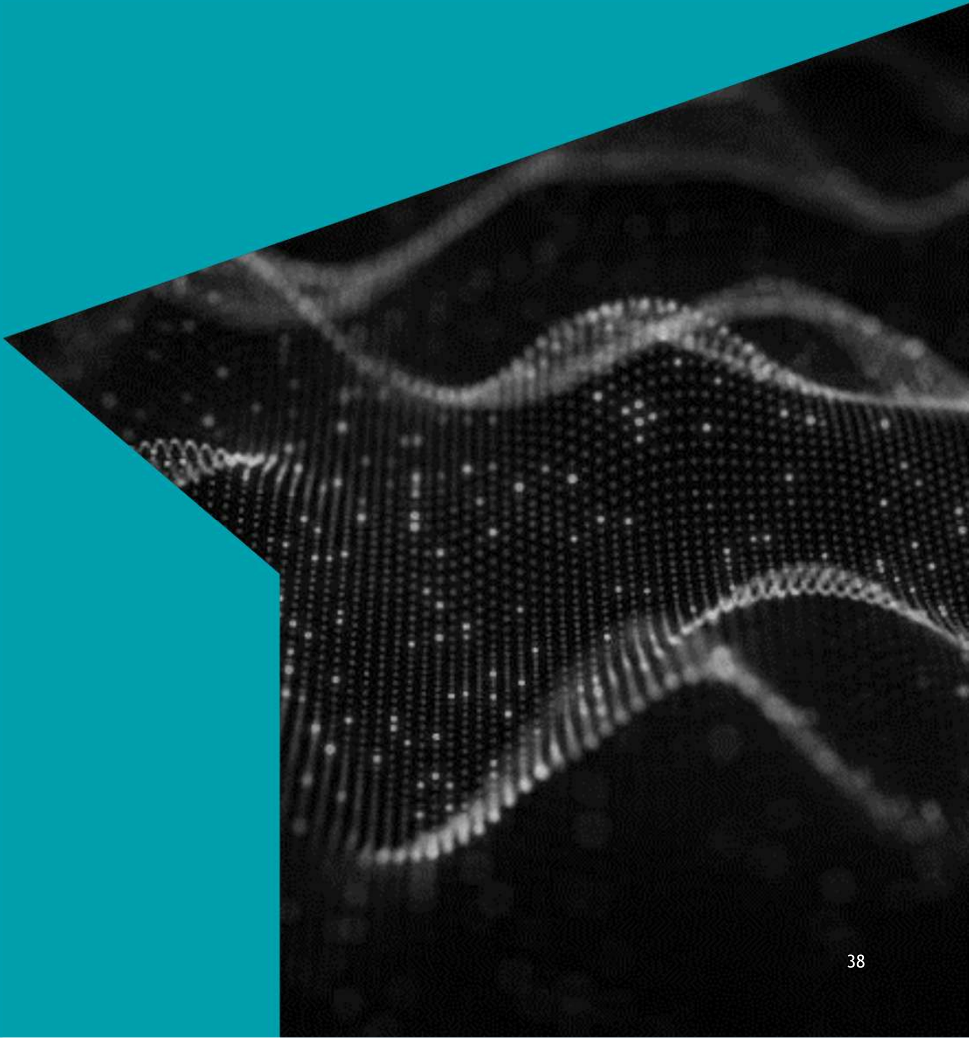
### Governance & Control Gaps

- No clear ownership or accountability for AI systems across the lifecycle.

- Lack of model inventory, risk classification, or escalation pathways.

- Inconsistent documentation across legal, security, product, and compliance teams.

# Takeaways



# Incident Response “Lessons Learned” and Best Practices - Checklist

### Governance & Readiness

❑ Assign a single incident commander with decision authority

❑ Pre-approve materiality and escalation thresholds (legal, board, regulators)

❑ Maintain an up-to-date incident response plan tied to real systems and vendors

### Detection & Scoping

❑ Ensure identity, cloud, and SaaS logs are retained and quickly accessible

❑ Practice first-24-hour scoping (what systems, what data, what access)

❑ Validate alerts across email, and collaboration platforms

### Containment & Technical Response

❑ Prioritize identity containment (disable tokens, rotate credentials, revoke sessions)

❑ Isolate affected systems without destroying forensic evidence

❑ Assume lateral movement and persistence until proven otherwise

### Legal, Privilege & Regulatory

❑ Engage counsel early to structure privilege from minute one

❑ Track regulatory notification timelines by jurisdiction and sector

❑ Document decisions contemporaneously (assume regulator review)

### Communications & Stakeholder Management

❑ Establish one internal source of truth for facts and updates

❑ Align legal, security, PR, and executive messaging before external statements

❑ Prepare for leaks, press, and customer questions before facts are final

### Third-Party & Supply Chain

❑ Identify which vendors have access to affected systems or data

❑ Trigger contractual notification and cooperation clauses immediately

❑ Validate vendor statements (do not rely solely on assurances)

### Ransomware & Extortion

❑ Separate business continuity decisions from payment negotiations

❑ Preserve evidence for law enforcement and insurance even if restoring

❑ Model impact of system shutdown vs. data exposure, not just ransom cost

### Recovery & Business Continuity

❑ Test restores before declaring recovery complete

❑ Monitor for re-entry and secondary extortion post-restoration

❑ Communicate clearly when systems are stable vs. merely online

### Post-Incident & Remediation

❑ Conduct an after-action review

❑ Convert findings into specific control changes, not policy updates

❑ Update training using what actually failed, not generic scenarios

# Litigation Avoidance Strategies

- Reduce exposure by:

1. **Documenting consent mechanics**
2. **Limiting third party data flows**
3. **Aligning cookie/pixel configurations with clear notices and opt outs**

- Strengthen data minimization and deletion practices to align with EDPB’s 2025 coordinated action on erasure (and to prevent over retention from becoming a damages narrative).

# AI Best Practices for 2026

**Testing, Monitoring & Auditing**

- Pre-deployment risk testing for accuracy, bias, and misuse scenarios.
- Ongoing performance monitoring, logging, and incident response playbooks.
- Periodic internal or third-party AI audits aligned to regulatory expectations.

**Procurement & Vendor Frameworks**

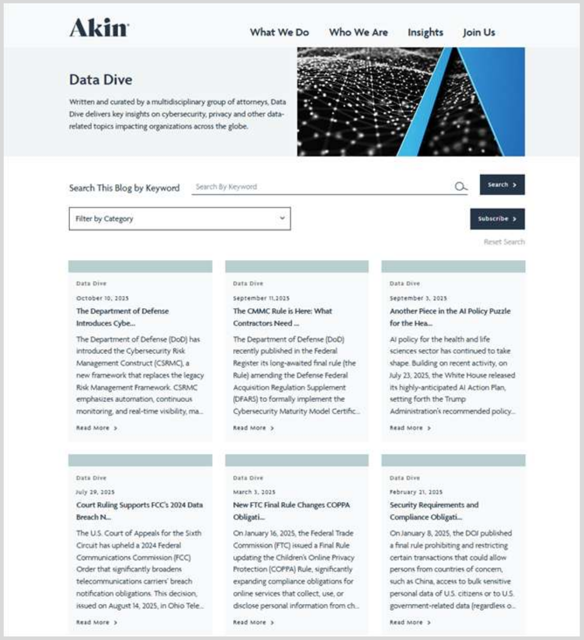
- Standardized AI procurement reviews covering training data sources, IP rights, security, and audit rights.
- Contractual controls on model updates, subcontractors, and data reuse.
- Clear allocation of responsibility for compliance failures and regulatory inquiries.

**Privacy-by-Design**

- Data minimization and purpose limitation embedded at model design stage.
- Segmentation of training, testing, and production data environments.
- Alignment of AI design choices with privacy notices, consumer rights, and regulatory risk assessments.

# Akin Resources

- Global and U.S. cybersecurity and privacy updates through Akin's AG Data Dive Blog and client alerts.



## Data Dive

Written and curated by a multidisciplinary group of attorneys, Data Dive delivers key insights on cybersecurity, privacy and other data-related topics impacting organizations across the globe.

Data Dive

October 10, 2025

**The Department of Defense Introduces Cybe...**

The Department of Defense (DoD) has introduced the Cybersecurity Risk Management Construct (CSRMC), a new framework that replaces the legacy Risk Management Framework. CSRMC emphasizes automation, continuous monitoring, and real-time visibility, ma...

Read More ›

Data Dive

September 11,2025

**The CMMC Rule is Here: What Contractors Need ...**

The Department of Defense (DoD) recently published in the Federal Register its long-awaited final rule (the Rule) amending the Defense Federal Acquisition Regulation Supplement (DFARS) to formally implement the Cybersecurity Maturity Model Certific...

Read More ›

Data Dive

September 3, 2025

**Another Piece in the AI Policy Puzzle for the Hea...**

AI policy for the health and life sciences sector has continued to take shape. Building on recent activity, on July 23, 2025, the White House released its highly-anticipated AI Action Plan, setting forth the Trump Administration's recommended policy...

Read More ›

Data Dive

July 29, 2025

**Court Ruling Supports FCC's 2024 Data Breach N...**

The U.S. Court of Appeals for the Sixth Circuit has upheld a 2024 Federal Communications Commission (FCC) Order that significantly broadens telecommunications carriers' breach notification obligations. This decision, issued on August 14, 2025, in Ohio Tele...

Read More ›

Data Dive

March 3, 2025

**New FTC Final Rule Changes COPPA Obligati...**

On January 16, 2025, the Federal Trade Commission (FTC) issued a Final Rule updating the Children's Online Privacy Protection (COPPA) Rule, significantly expanding compliance obligations for online services that collect, use, or disclose personal information from ch...

Read More ›

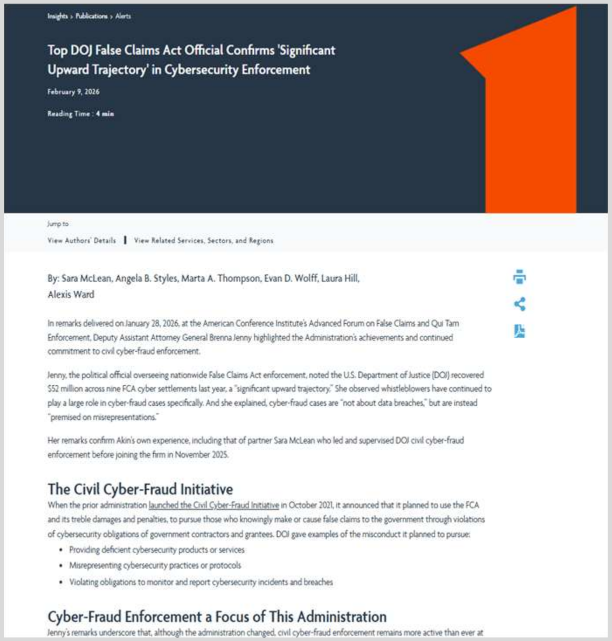
Data Dive

February 21, 2025

**Security Requirements and Compliance Obligati...**

On January 8, 2025, the DOJ published a final rule prohibiting and restricting certain transactions that could allow persons from countries of concern, such as China, access to bulk sensitive personal data of U.S. citizens or to U.S. government-related data (regardless o...

Read More ›


Insights › Publications › Alerts
Jump to
View Authors' Details
View Related Services, Sectors, and Regions

## Top DOJ False Claims Act Official Confirms 'Significant Upward Trajectory' in Cybersecurity Enforcement

February 9, 2026

Reading Time : **4 min**

By: Sara McLean, Angela B. Styles, Marta A. Thompson, Evan D. Wolff, Laura Hill, Alexis Ward

In remarks delivered on January 28, 2026, at the American Conference Institute's Advanced Forum on False Claims and Qui Tam Enforcement, Deputy Assistant Attorney General Brenna Jenny highlighted the Administration's achievements and continued commitment to civil cyber-fraud enforcement.

Jenny, the political official overseeing nationwide False Claims Act enforcement, noted the U.S. Department of Justice (DOJ) recovered $52 million across nine FCA cyber settlements last year, a "significant upward trajectory." She observed whistleblowers have continued to play a large role in cyber-fraud cases specifically. And she explained, cyber-fraud cases are "not about data breaches," but are instead "premised on misrepresentations."

Her remarks confirm Akin's own experience, including that of partner Sara McLean who led and supervised DOJ civil cyber-fraud enforcement before joining the firm in November 2025.

### The Civil Cyber-Fraud Initiative

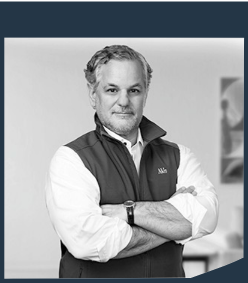
When the prior administration launched the Civil Cyber-Fraud Initiative in October 2021, it announced that it planned to use the FCA and its treble damages and penalties, to pursue those who knowingly make or cause false claims to the government through violations of cybersecurity obligations of government contractors and grantees. DOJ gave examples of the misconduct it planned to pursue:

- Providing deficient cybersecurity products or services
- Misrepresenting cybersecurity practices or protocols
- Violating obligations to monitor and report cybersecurity incidents and breaches

### Cyber-Fraud Enforcement a Focus of This Administration

Jenny's remarks underscore that, although the administration changed, civil cyber-fraud enforcement remains more active than ever at

# Team Contact Information

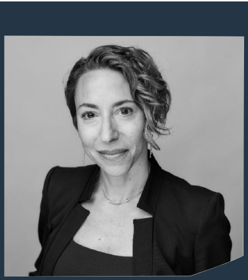


**Evan Wolff**
Partner

ewolff@akingump.com
Washington
+1 202.887.4104

**Rita Heimes**
Senior Counsel

rheimes@akingump.com
Washington
+1 202.887.4165



**Erica Bomsey**
Senior Vice President and Deputy General Counsel

erica.r.bomsey@leidos.com
Washington
Leidos

**Anthony T. Pierce**, *Moderator*
Partner

apierce@akingump.com
Washington, D.C.
+1 202.887.4411