November 12, 2025

How Vendors Can Become Your Liability

Amy Pimentel
McDermott Will & Schulte

Shannon Ralich
Machinify

Siri Swayampu
Lowe's Companies

Tien Pham
FINRA

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Amy Pimentel

Partner
McDermott Will & Schulte

Shannon Ralich

Vice President of Compliance and Chief Privacy Officer
Machinify

Siri Swayampu

Technology & Cyber Counsel
Lowe's Companies

Tien Pham

Principal Counsel & Associate Director, Enterprise Data Privacy Office - OGC
FINRA

Framing the Issue

Privacy+ Security Forum

Vendors and increasingly at the epicenter of privacy and security failures

- Once “back-end processors,” now frontline **risk points**
- Legal liability follows the data supply chain
- Regulators increasingly penalize vendor failures
- Private lawsuits are expanding this exposure
- Privacy missteps = financial + reputational damage

Agenda

Privacy+ Security Forum

Overview:

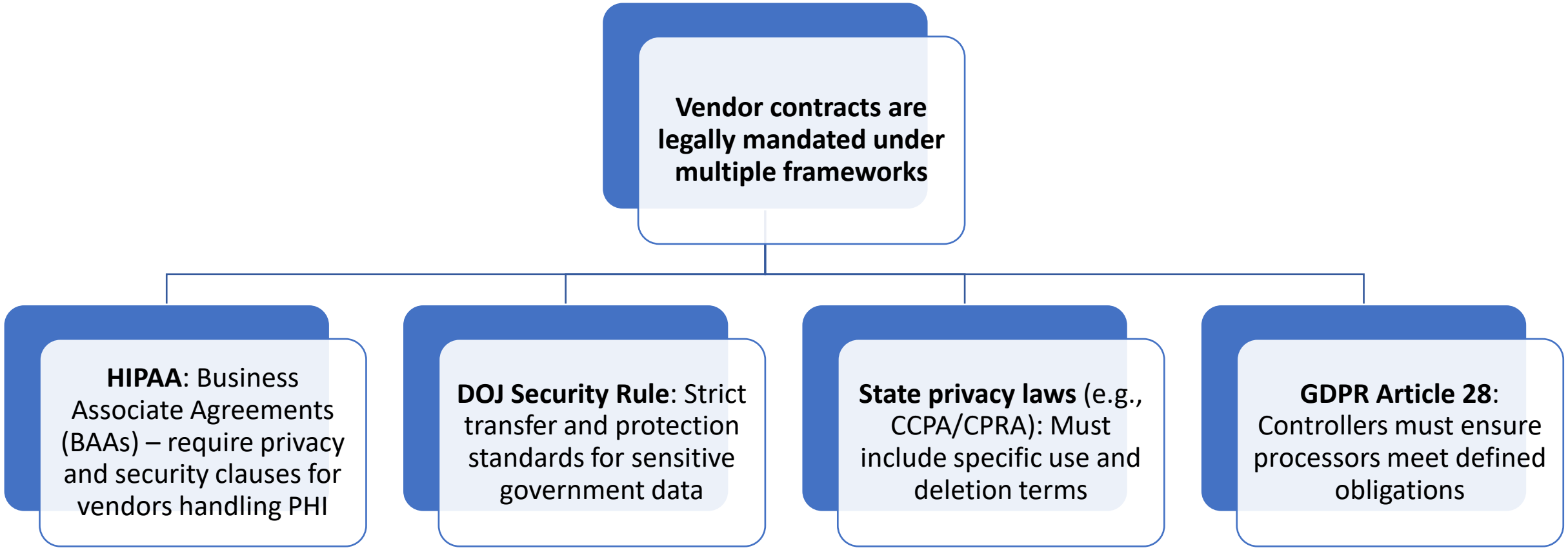
- Regulatory Framework
- Legal Exposure and Enforcement Trends
- Case Studies: Regulatory Enforcement and Vendor Failures
- Legal Risk Pathways via Vendors
- New Classes of Risk in the AI and AdTech Vendor Landscape
- Key Practice Takeaways
- Strategic Outlook and Conclusions
- Q&A

Regulatory Framework

Controller Responsibility and Vendor Oversight

Privacy+ Security Forum

Contractual Requirements



Vendor Oversight

Privacy+ Security Forum

The Expanding Compliance Perimeter

- **State security laws** mandate oversight of third-party vendors (e.g., MA Data Security Reg., NYDFS 23 NYCRR 500.11)
- **Regulators now expect proof** of sub-processor management and cross-border data controls
- **Financial sector rules** (GLBA Safeguards, Reg S-P) require continuous vendor risk governance

Assignment of Liability

Privacy+ Security Forum

When Your Vendor's Failure Becomes Yours

- **GDPR**: Controllers remain fully liable for processor failures
  - Article 28: "Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."
- **Joint controller liability** is increasingly recognized
- **EU AI Act**: Shared responsibility across the AI value chain

Legal Exposure and Enforcement Trends

Privacy+ Security Forum

Recent Priorities and Trends

Privacy+ Security Forum

- Federal
  - Past 3 months, themes from enforcement actions, press releases, public statements, reports
    - Children's privacy and safety (Disney, Apitor, Aylo, SendIt App)
    - Companion chatbots (*September FTC Inquiry*)
    - Misleading and deceptive conduct (*Aylo*)
    - Data transfer outside of the US (*Apitor)*
    - Charging individuals (*Amazon Prime*)

Cross-Regulatory Collaboration

Privacy+ Security Forum

States

- State AGs + CPPA + FTC increasingly coordinating on privacy enforcement (SendIt App; Aylo – FTC and Utah)
- Focus on no or inadequate disclosure of a consumer's rights, no or inadequate mechanisms for consumers to opt out or otherwise exercise their rights; failing to action on opt-outs; and data brokers
- Expectation of strong governance before violations occur
- Expectation of collaboration between states and controllers on compliance
- Fines appear generally to be decreasing, but this may not be permanent
- Examples of recent enforcement actions:
  - DoorDash – contract failures under the CCPA
  - Todd Snyder – failure to oversee AdTech vendors

Vendor liability implications

- Continued scrutiny on contracts, vendors, and processing purposes – not just breaches
- Controllers remain liable for vendor errors under CCPA and GDPR principles
- “Head in the sand” approach will not shield organizations
- Respond to consumer complaints as *early indicators of vendor risk*
- Key analytical questions:
  - What did you know, and when?
  - What actions did you take?
  - Was there consumer harm?

Evolving Legal Risk

Privacy+ Security Forum

Evolving Risks

Privacy+ Security Forum

Missing required contract terms	Gaps create uncertainty in obligations, liability, and enforcement
Operational misalignment, particularly with backups/archives	Lack of technical enforcement (no API integration for DSARs, access limits, or audit logs)
Breach notification failures	Missed coordination = regulatory exposure and consumer harm
Battle of the lingo and buzzwords	Legal and technical teams interpret risk differently, creating blind spots in due diligence and compliance reviews

New Classes of Risk in the AI Vendor Landscape

Privacy+ Security Forum

Data Use Uncertainty

Privacy+ Security Forum

AI Data Use: The Black Box Problem

- Hard to verify **how vendors store, process, or reuse input data**
- Customer data may be used for:
  - Model training or fine-tuning (unexpected reuse)
  - Derivative tools or prompt mining
- **Practice Tips:**
  - Map your data flow
  - Ask vendors *where*, *how*, and *for how long* data is stored
  - Update internal risk assessments regularly
  - Identify all sub-processors (third → fifth party)

Model Inference & Re-Identification

Privacy+ Security Forum

When Anonymized Data Isn't Safe

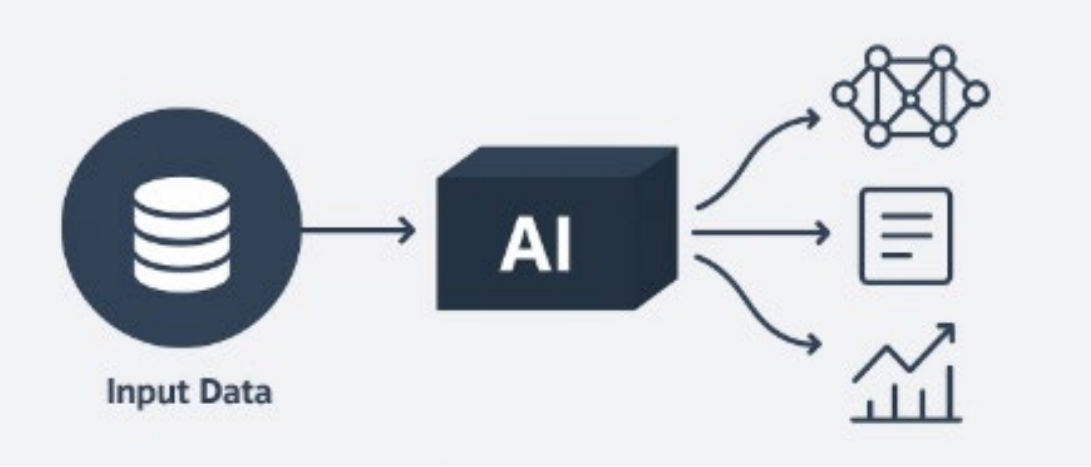
- AI outputs can reveal or infer sensitive traits
- Pattern recognition may re-identify individuals
- Traditional "de-identification" safe harbors (CCPA/HIPAA) no longer guarantee privacy
- **Practice Tips:**
  - Include **AI-specific contract terms**
  - Add **AI Addendum** for vendor agreements
  - Track **what your business inputs into AI tools**

Uncontrolled Data Retention & Shadow Copies

Privacy+ Security Forum

AI Systems Do Not Forget

- Vendor APIs often **cache, log, or retain** prompts by default
- Retained data can resurface in **training or model refinement**
- **Practice Tips:**
  - Confirm data deletion and retention timelines
  - **Use contractual language** to prohibit reuse



Security Vulnerabilities

Privacy+ Security Forum

Emerging AI Attack Vectors

- **Prompt Injection:** Manipulating model responses
- **Model Inversion**: Reconstruction sensitive data from outputs
- **Data Poisoning**: Corrupting training data
- **Multi-Tenancy Risks**: Weak isolation in hosted AI environments
- **Practice Tips:**
  - Work with IT/Security to assess AI vendor environments
  - Require incident reporting & security certifications

New Classes in the AdTech Vendor Landscape

Privacy+ Security Forum

Data Shared Across Contexts

Privacy+ Security Forum

Tracking Without Boundaries

- AdTech vendors track users across **sites, devices, and apps**
- Data often used beyond **original consent or context**
- Cookies, pixels, and device IDs enable cross-context profiling
- Risks: unlawful “sale/share” under CCPA + erosion of trust

Misclassification of Vendors

Privacy+ Security Forum

Service Provider or Third Party? It Matters!

- Mislabeling AdTech vendors creates compliance exposure
- Wrong classification = missed **notice and opt-out** obligations
- Triggers **contractual and enforcement gaps**
- Especially critical for data sharing and marketing analytics

Inadequate Contractual Controls

Privacy+ Security Forum

Contracts Cannot Be Afterthoughts

- Many legacy AdTech contracts allow:
  - Cross-client user profiling
  - Data resale/enrichment
  - Combining with sensitive categories
- Missing **key CCPA/CPRA** terms (use limits, audit rights, retention limits)

Invisible Sub-processors and Data Brokers

Privacy+ Security Forum

The Hidden Web of Data Sharing

- AdTech vendors often share data downstream to **unknown partners**
- Controllers lack full **data lineage visibility**
- Results in unintentional “sale/share” violations
- Major reputational and enforcement risk

Best Practices for Legal and Compliance Functions

Privacy+ Security Forum

Vendor Life Cycle Management

Privacy+ Security Forum

Know	Discover	Track	Train	Refresh
Know Your Vendors	Use tailored diligence questionnaires mapped to legal obligations (CCPA, GDPR, HIPAA)	Track vendor onboarding + data flow in central inventory Document compliance diligence and business decisions	Implement training for contracting infosec/IT teams	Periodically review and refresh vendor agreements to capture add on services and changes in risk and law

Contract Optimization

Privacy+ Security Forum

Strengthen Your Contracts

- Build **cross-functional strategies** with legal, IT, and procurement
- Reevaluate terms during renewal – not just at onboarding
- Ensure contracts:
  - Contain key clauses
  - Restrict secondary use/sale
  - Include real-time monitoring and audit rights
- Tips:
  - Add definitions
  - Use negotiations as a second diligence step
  - Add AI Addendum if vendor uses or integrates AI tools
  - Be cautious when playbooking

Focus on High-Risk Vendors (Especially AI)

Privacy+ Security Forum

Focus Where it Matters Most

- Pay extra attention to **AI Vendors**:
  - Ensure no model training on enterprise/consumer data without consent
  - Protect IP + confidentiality in generative or predictive modeling
  - Require detailed **Technical and Organizational Measures (TOMs)**

Monitor and Audit

Privacy+ Security Forum

Keep Watch After the Ink Dries

- Conduct **periodic reviews** of high-risk vendors
- Apply **technical enforcement** (tagging, access control)
- Act quickly when vendor behavior or product design crosses boundaries
- Document **advice to business** and risk acceptance decisions

Strategic Outlook and Conclusions

Privacy+ Security Forum

Vendor Risk is the New Regulatory Frontier

- Vendors are now **regulatory touchpoints**, not just operational partners
- Regulators view **vendor governance as proof of privacy maturity**
- Legal teams **must embed with procurement and security** to manage real risk
- What is “reasonable” varies: **industry context shapes expectations**
- Education internal stakeholders: **vendor compliance = legal defense**
- Vendor failures can **shift regulatory and litigation exposure upstream**

Q&As

Privacy+ Security Forum

Contact Information

Privacy+ Security Forum

Amy Pimentel

apimentel@mwe.com
McDermott Will & Schulte

Shannon Ralich

Shannon.ralich@machinify.com
Machinify

Siri Swayampu

Siri.swayampu@lowes.com
Lowe's Companies

Tien Pham

Tien.Pham@finra.org
FINRA