ACC Association of Corporate Counsel

NATIONAL CAPITAL REGION

SOFTWARE LICENSING, SAAS AND DATA AGREEMENTS

Contracting Challenges in the Evolving Digital Ecosystem

September 30, 2025

A POINT OF VIEW
LIKE NO OTHER

WOMBLE BOND DICKINSON

Mervin A. Bourne, Jr.

Senior Counsel – Cybersecurity, Privacy & AI
Pacific Gas and Electric

Tara N. Cho, CIPP E/US

Partner – Chair, Privacy & Cybersecurity
Womble Bond Dickinson

CONTINUED LEGISLATION

2018

EU GDPR becomes effective

CCPA is enacted in CA

CCPA effective

CPRA passed by ballot initiative to amend CCPA

VCDPA enacted in VA March 2021

CPA enacted in CO July 2021

UT and CT state privacy laws enacted

Amended CCPA effective

VA, CO, CT, UT privacy laws effective

CONTINUED LEGISLATION

2024

EU AI Act enacted

Utah Artificial Intelligence Policy Act effective (first state AI-centric law)

FL, OR, TX, MT privacy laws effective

2025

Privacy laws in DE, IA, MD, MN, NE, NH, NJ, TN become effective

Amended UT AI law effective

EU Data Act effective

2026

CO Artificial Intelligence Act becomes effective

IN, KY, RI privacy laws become effective

CCPA risk assessments begin

2027

Compliance deadline for ADMT requirements under CCPA

2028

CCPA cybersecurity audit requirement begins

2026-2027 CCPA risk assessments due to CPPA

US DIGITAL LANDSCAPE

- Federal Privacy (sector- and data specific FTC Act, COPPA, HIPAA, GLBA)
  60+ Federal privacy bills proposed in the 2023-2024 Congress*, more targeted, narrower scope than comprehensive

- State Privacy
  20 comprehensive state privacy laws enacted – more amendments and privacy and AI-adjacent legislation across states

- International Privacy
  The EU member countries and UK among the 79% of countries worldwide with privacy and data protection laws[1]

[1] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

US DIGITAL LANDSCAPE

- Security
  State safe harbor security laws and patchwork of security standards across federal sector requirements and voluntary industry standards

- Data Breach
  Varying timelines between sector-specific federal requirements and state laws requirements across all 50 states and territories versus critical infrastructure and government contract standards

- Processing Activity and Data Specific
  Data broker laws; precise geolocation tracking; text messaging and marketing; website operations; automated decision-making; biometric data laws; consumer health data laws; AI laws; digital replica / deep-fake laws, special requirements for “sensitive data”

KEY PRIVACY REQUIREMENTS (INITIALLY)

Key emphasis of state privacy laws is consumer protection.

- Even if primarily business-to-business (B2B), the California privacy law (CCPA) applies to B2B data and employee and job applicant data much like the EU GDPR
- Individual rights of data subjects is also more similar to GDPR, including:
  - Right to delete
  - Right to access / data portability
  - Right to amend / correct
  - Right to limit use of sensitive personal information
  - **Right to opt out of sales or sharing** (this includes sharing of personal information like IP address and session or browser information collected from pixels, cookies or other online trackers for targeted or behavioral advertising and certain types of analytics)
- Global Privacy Controls / Universal Opt-Out Mechanisms Required (where browser can send a signal to a website not to track the visitor so no trackers fire from the moment the person lands on the site)

EVOLVING PRIVACY REQUIREMENTS (NOW)

Fluid requirements under state and federal standards resulting in potentially conflicting emphasis on innovation and economic growth versus consumer protections

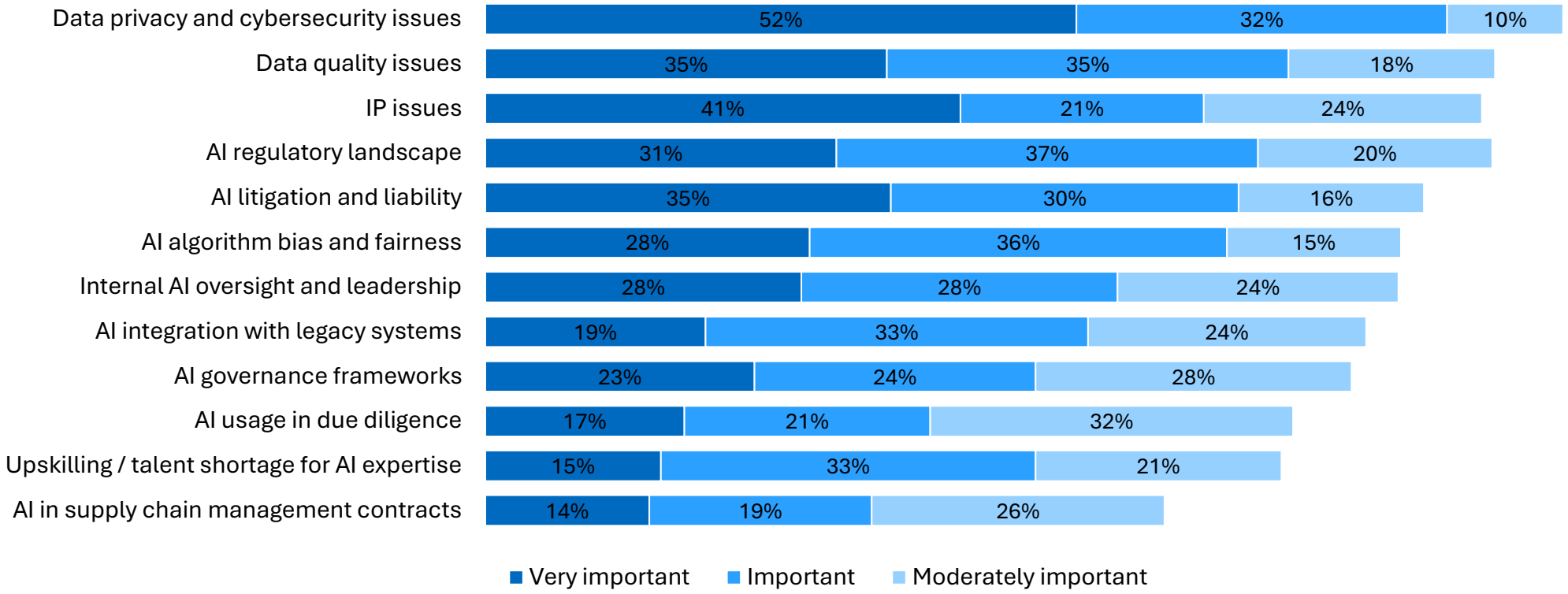
- Bi-partisan agreement on protecting children and teens
- Federal emphasis on international dominance in the era of AI vs. many states pushing for risk-based AI models and more stringent data privacy standards akin to the EU manner of fundamental rights
- Just in time notices and complex consents create UX friction that can stifle innovation or require business risk acceptance to stay competitive
- Intersecting requirements across states and federal sectors often require governance models around the most stringent standards
- Even the most seemingly compliant digital assets are still targets of nuisance litigation

ARTIFICIAL INTELLIGENCE

United States	European Union
“America’s AI Action Plan”	EU AI Act
Innovation-forward / reducing “red tape”	Risk-based model
Win the AI race	Some outright prohibitions
Mix of federal agency enforcement	Comprehensive framework across EU
Innovation, growth, research	Transparency, trust, fundamental rights
	

IMPORTANCE OF AI TOPICS TO BUSINESS AND LEGAL NEEDS

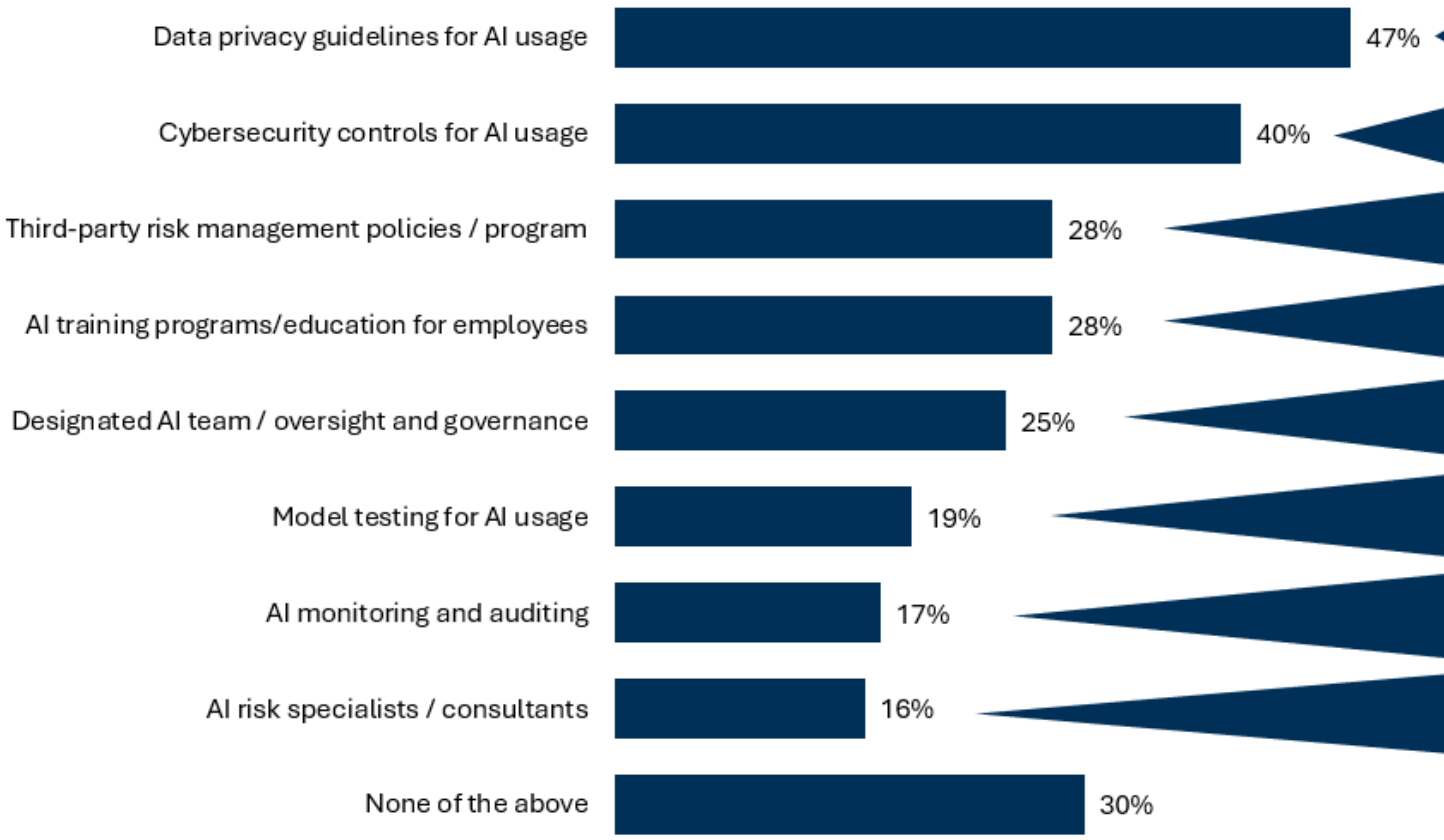
What level of importance would you place on insights and guidance related to the following AI topics in terms of how they affect your business and legal needs?



Source: “The View from the Top: How Business Leaders are Operationalising AI”, Womble Bond Dickinson Whitepaper, Spring 2025.

AI ACTIONS TAKEN

Which of the following, if any, does your company have in place? Please select all that apply:



	Industry	%
High	Manufacturing	88%
Low	Technology / Telecom / Software	44%
High	Manufacturing	88%
Low	Professional Services	25%
High	Financial Services / Banking	57%
Low	Energy and Natural Resources	0%
High	Healthcare and Life Sciences	50%
Low	Technology / Telecom / Software	19%
High	Energy and Natural Resources	60%
Low	Professional Services	0%
High	Healthcare and Life Sciences	40%
Low	Energy and Natural Resources	0%
High	Financial Services / Banking	43%
Low	Energy and Natural Resources	0%
High	Healthcare and Life Sciences	38%
Low	Real Estate	0%

Source: “The View from the Top: How Business Leaders are Operationalising AI”, Womble Bond Dickinson Whitepaper, Spring 2025.

PRIVACY ENFORCEMENT HIGHLIGHTS

California, Texas, Virginia, and New Hampshire AGs have dedicated privacy unit for enforcement. The FTC is also focused on unfair and deceptive practices for website and app operators involving online trackers, opt outs and dark patterns.

California Enforcement Actions (all related to global privacy controls, online tracking and targeted advertising)

- Sephora – $1.2M fine (2022)
- Google – $93M+ injunctive terms / increased transparency and disclosures (2023)
- DoorDash – $375K (violations of CCPA and CalOPPA) (2024)
- Honda - $632,500 (CCPA) (2025)
- Healthline Media - $1.55M (CCPA) (2025)

California Compliance Letters

- Sweep of online retailers for advertising and analytics tools without opt-out mechanism and no service-provider terms; no GPC
- Notice at Collection (timing and placement)
- Dark Patterns and Data Minimization (CPPA Enforcement Advisory)

New York AG Privacy Guides

- AG issued guidance on use of cookies, online tracking and targeting on websites
- No comprehensive state privacy law but enforceable under consumer protection laws

Multi-State Actions

- September 9, 2025 CA, CO, and CT AGs announced a joint investigative sweep to investigate businesses refusing to honor opt-out of sale preferences
- Evaluating GPC deployment

LITIGATION TRENDS

There has been a rapid increase in arbitration demands, demand letters, and class action litigation associated with the use of online trackers such as pixels and cookies. These claims vary by state and can be alleged despite a website that fully complies with state privacy laws.

- Common website functionality involved in the alleged claims
  - Online tracking pixels, cookies and similar tools
  - Chatbots
  - Session replay tools
  - Embedded video content with trackers

- Recent CIPA settlements have involved monetary relief of:
  - $115M (Oracle, 2024)
  - $50M (Fifth Third Bank and vendor, 2022)
  - $19.5M or $680 per consumer (Wells Fargo and vendor, May 2025)
  - $3.4M (fuboTV, 2025)
  - Other settlements in response to pre-litigation demand letters can range from $10K to six-figure settlement amounts even before a formal claim is filed

- Cyber insurance impact (recent insurance applications include an entire section of questions about whether the organization has received these types of demands or been involved in pixel litigation)

LITIGATION TRENDS – COMMON CLAIMS

- California Invasion of Privacy Act (CIPA) and other state's equivalent wiretap laws (PA, WA, MA)
  - Decades-old criminal statute enacted in 1967 to prevent eavesdropping on telephone calls and pen registers without consent.
  - Plaintiffs allege that tracking technologies are used to "record" a user's interactions with websites, which amounts to the use of a "pen register" or "trap and trace" device.
  - Plaintiffs allege that pixels active on chatbots amount to a wiretapping by a third party.
  - Under California law, explicit consent is required to use a pen register or trap and trace device.

- Song-Beverly Act (CA and ~14 other states)
  - Designed to protect consumers from disclosing personal information at the checkout counter, Song-Beverly is now being applied to online checkouts.
  - Plaintiffs allege that the defendant's use of pixel technologies to collect IP addresses and other personal information violates Song-Beverly.
  - Lawsuits are currently active in California and Massachusetts, with 12 other states having similar laws.
  - Both California and Massachusetts include statutory damages.

- Video Privacy Protection Act (VPPA)
  - Law from 1998 that prohibits the disclosure of video rental records containing personally identifiable information.
  - Plaintiffs allege that the use of various pixels and tracking technologies on websites with embedded videos violates the VPPA by collecting information on whether the consumer watched the video and their personal information.
  - Plaintiffs allege the use of various pixels and tracking technologies on websites with embedded videos amounts to VPPA by collecting if the consumer watched the video and their personal information.
  - Commonly alleged where website has embedded videos of any kinds, which typically have Youtube or other trackers attached.

STRATEGIES FOR MITIGATING COMPLIANCE & LITIGATION RISK

1. Privacy Notices & Disclosures
• Ensure privacy policies are clear, accurate, and up-to-date....

2. Opt-Out Mechanisms
• Implement functional opt-out tools for data sale/sharing....

3. Cookie & Tracking Technologies
• Deploy compliant cookie banners with granular consent options....

4. Consumer Rights Fulfillment
• Respond to consumer requests (access, deletion, correction) within legal timelines....

5. Vendor & Third-Party Contracts
• Review contracts for proper data processing and privacy terms....

6. Technical & Legal Audits
• Conduct regular privacy audits of websites, apps, and backend systems....

7. Defensive Documentation
• Maintain records of privacy policy updates and consumer notices....

8. Staff Training & Awareness
• Train staff on privacy laws and consumer rights...

9. Litigation Preparedness
• Monitor enforcement trends and litigation risks....

CONTRACTING STRATEGIES – AI AND IP TERMS

- Use for AI Training
  - What type of data – if any – can be used for AI training (anonymized, aggregated)
  - Prohibitions on use for training
- Ownership of outputs
  - Who owns the outputs?
  - Can the provider reuse or leverage that output for other customers?
- Liability and Indemnification (for errors, bias, or IP infringement)
- Data Limits (can PII be inputted, IP protections)

CONTRACTING STRATEGIES – AI AND IP TERMS

- Reps and Warranties
  - Accuracy and reliability of the AI system (training, testing, event logging, transparency, compliance with law)
  - Bias and fairness (and degree of human oversight required), particularly for high-risk use cases
- Regulatory Compliance
  - Require compliance with AI-specific regulations
  - Mandate on-going updates to practices and guidance evolve

CONTRACTING STRATEGIES – DATA TERMS

- Data Ownership and Use
  - Clear provisions on data ownership and limitations on uses and disclosures (prevent “sales”)
  - Consider value of de-identified or aggregate data
- Personal Data Limits
  - Cross-border transfers
  - DOJ bulk data transfer rules
  - Security requirements
  - Breach notification timing and costs
- Sub-processors and Downstream Obligations
  - Be cautious of what is mandated downstream as subcontractor agreements may already be in place and / or non-negotiable
  - Don’t think that hiding behind a tech giant insulates the business from risk or liability (e.g., CSPs, major CRM or marketing providers, etc.)

COMMON “GOTCHA” PROVISIONS

- Scope and term of the agreement
  - Watch for “and affiliates” language that can result in unintended consequences and risk – particularly for broader data disclosures to related entities not party to the agreement as well as software providers owing duties not just to the counterparty but “affiliates”
  - Ensure survival provisions consider data protection requirements, particularly if regulated data are maintained post-termination or in system back-ups
- Liability
  - Carefully navigate liability carve-outs and limitations to ensure all digital risk is addressed
  - Consider the organization’s insurance protections and limits as some policies may prohibit certain levels of indemnity and liability exposure in contracting
- Anticipate Future Value
  - If high-volumes of data (even aggregate data) are involved, consider the commercial implications and value of the data to the counterparty

VENDOR / PROCUREMENT AND CONTINGENT WORKERS

- **Vendor Selection and Due Diligence**
- **Contractual Safeguards**
- **Technical Controls and Monitoring**
- **Documentation and Recordkeeping**
- **Litigation Preparedness**

QUESTIONS

WOMBLE
BOND
DICKINSON