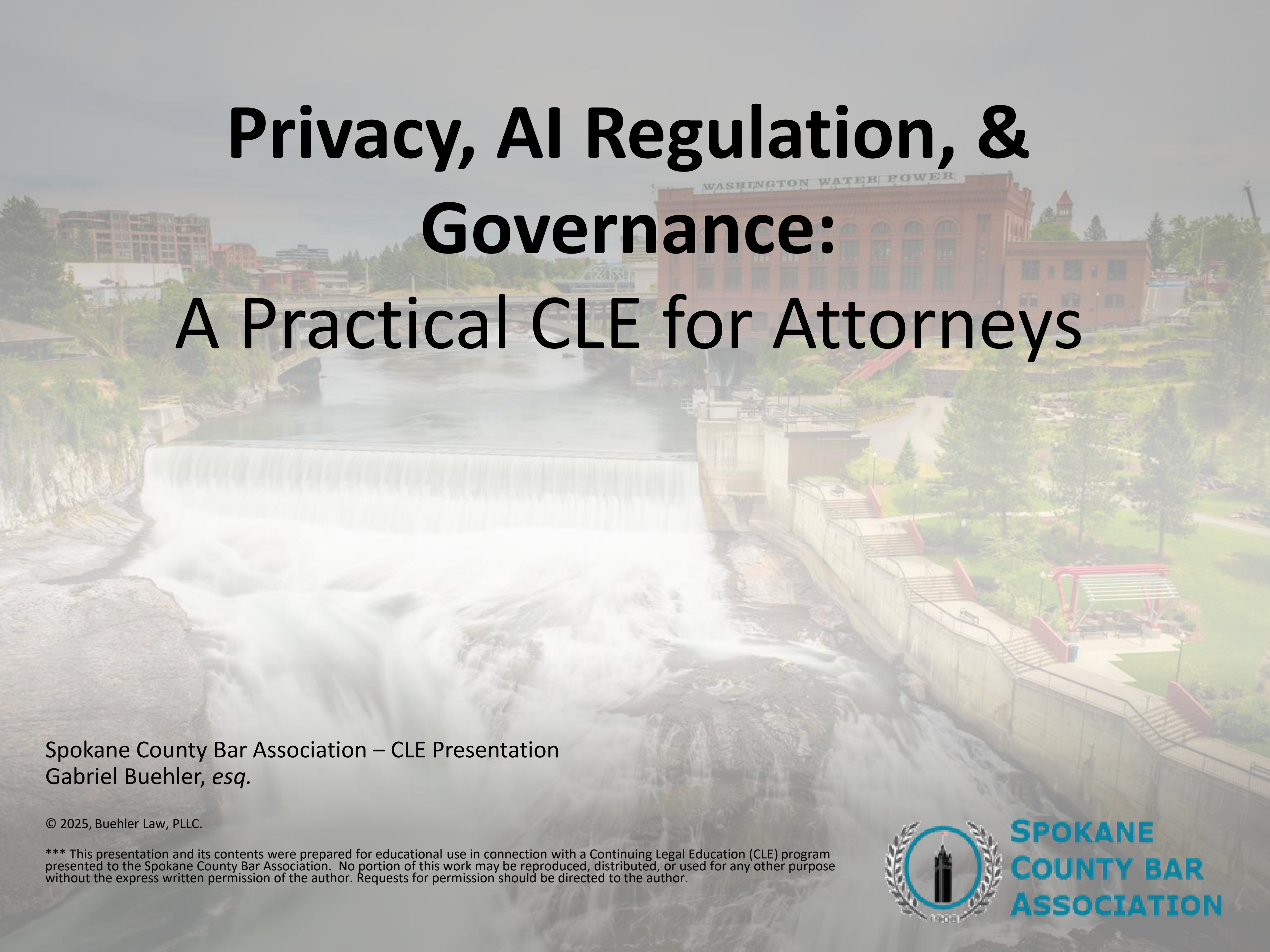


Privacy, AI Regulation, & Governance:

A Practical CLE for Attorneys

Spokane County Bar Association – CLE Presentation
Gabriel Buehler, *esq.*

*** This presentation and its contents were prepared for educational use in connection with a Continuing Legal Education (CLE) program presented to the Spokane County Bar Association. No portion of this work may be reproduced, distributed, or used for any other purpose without the express written permission of the author. Requests for permission should be directed to the author.

Spokane
County Bar
Association

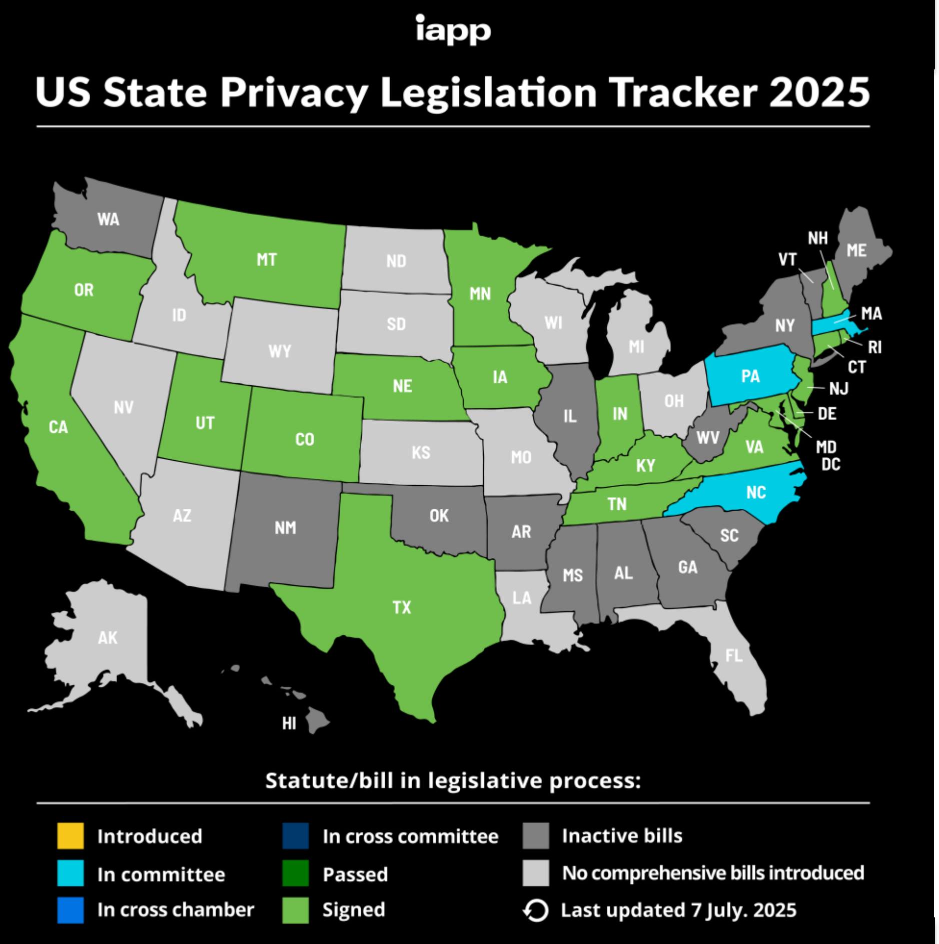
Gabriel Buehler

- Owner, Buehler Law, PLLC
  - Business, Privacy, and Technology Law
- Inhouse Legal Counsel, Pipl Inc & Elephant
  - Fraud and Risk B2B, Data Broker
- WSBA ABA House of Delegates
- ABA Committee Vice-Chair
  - TIPS BLC
  - CyberSecurity, Data Privacy, and AI
  - Technology & New Media
  - Media, Privacy, & Advertising
  - Corporate & Inhouse Counsel

Agenda

- Introduction to U.S. & International Privacy Law
- Emerging AI Regulation
- AI Governance for Organizations
- AI in the Legal Industry
- Prompt Engineering
- Enterprise-Grade AI Solutions
- Q&A / Closing Remarks

*Disclaimer – This presentation and its accompanying materials are provided solely for educational purposes in connection with a Continuing Legal Education (CLE) program. They are **not intended as legal advice and do not create an attorney–client relationship.** Participants should consult qualified counsel regarding specific legal or regulatory matters applicable to their circumstances.



Why Privacy Law Matters Now

Explosion of personal data, AI systems ingesting data, regulatory risk

Client confidentiality risks; professional responsibility; vendor due diligence

Patchwork of state and sectoral laws in the U.S.

Comprehensive U.S. Privacy Laws

Landscape Summary

No single federal omnibus privacy law

California Consumer Privacy Act (CCPA/CPRA)

Sectoral:

GLBA

(financial institutions)

HIPAA

(healthcare)

Washington

My Health My Data Act (MHMD)

GDPR & CCPA/CPRA

The Gold Standards of Privacy Laws in a Glance

Category	**GDPR (General Data Protection Regulation)**	**CCPA / CPRA (California Consumer Privacy Act / California Privacy Rights Act)**
Enactment & Effective Date	Adopted April 2016; effective **May 25, 2018** across the European Union.	Enacted **June 2018**, effective **January 1, 2020**; expanded by **CPRA effective January 1, 2023**.
Purpose	Creates a uniform, comprehensive framework for **data protection and privacy rights** across the EU.	Establishes **consumer privacy rights** for California residents and regulates business data practices.
Who It Applies To	Applies to **controllers and processors** that process personal data of individuals in the EU, even if the organization is outside the EU.	Applies to **for-profit businesses** doing business in California meeting thresholds: >$25M revenue, or data of ≥100,000 consumers/households, or ≥50% revenue from selling/sharing data.
Scope of Data	Covers any **personal data** that can identify an individual (broadly defined).	Covers **personal information** about California residents, households, or devices.
Key Obligations	Requires **lawful basis** for processing, transparency, data subject rights, DPIAs, breach notification, and data protection by design/default.	Requires **notice at collection**, honoring of **consumer rights (access, delete, opt-out, correct)**, data minimization, and contractual limits on data sharing.
Enforcement Authority	National **Supervisory Authorities** in each EU member state, coordinated by the European Data Protection Board (EDPB).	**California Attorney General** and **California Privacy Protection Agency (CPPA)** enforce compliance; limited private right of action for data breaches.
Penalties for Noncompliance	Up to **€20 million or 4% of global annual revenue**, whichever is higher.	Up to **$2,500 per violation** or **$7,500 per intentional violation**; private damages **$100–$750 per consumer per incident** for breaches.
Territorial Reach	Global—applies extraterritorially to non-EU entities targeting or monitoring EU residents.	Primarily domestic—applies to businesses that collect or sell personal information of **California residents**.

GDPR – Key Duties - Controllers

Duty	Description	GDPR Reference
Lawfulness, Fairness, Transparency	Must process data lawfully, fairly, and transparently; establish lawful basis for processing (consent, contract, etc.).	**Art. 5(1)(a); Art. 6**
Purpose Limitation	Collect for specified, explicit, legitimate purposes; not further process incompatibly.	**Art. 5(1)(b)**
Data Minimization	Limit processing to what is necessary for stated purposes.	**Art. 5(1)(c)**
Accuracy	Keep data accurate and up to date.	**Art. 5(1)(d)**
Storage Limitation	Retain personal data only as long as necessary.	**Art. 5(1)(e)**
Integrity & Confidentiality	Ensure appropriate security, including protection against unauthorized or unlawful processing.	**Art. 5(1)(f); Art. 32**
Accountability Principle	Must be able to demonstrate compliance with all GDPR principles.	**Art. 5(2)**
Transparency to Data Subjects	Provide clear information in privacy notices at collection or when obtained indirectly.	**Arts. 12–14**
Facilitation of Data Subject Rights	Enable rights requests (access, rectification, erasure, restriction, portability, objection).	**Arts. 15–22**
Record-Keeping	Maintain records of processing activities.	**Art. 30(1)**
Data Protection by Design & Default	Integrate data protection measures into processing activities.	**Art. 25**
Data Protection Impact Assessments (DPIA)	Conduct DPIA for high-risk processing.	**Art. 35**
Breach Notification	Notify supervisory authority within 72 hours; data subjects if high risk.	**Arts. 33–34**
Processor Oversight & Contracts	Use only processors providing sufficient guarantees; have written DPA.	**Art. 28(1), (3)**
International Transfers	Ensure transfer mechanism (adequacy, SCCs, BCRs, etc.).	**Arts. 44–49**
Designation of DPO (if required)	Appoint DPO if core activities involve large-scale monitoring or special categories.	**Arts. 37–39**

GDPR – Key Duties - Processors

Duty	Description	GDPR Citation
Process Only on Controller Instructions	Cannot process for own purposes.	**Art. 29; Art. 28(3)(a)**
Confidentiality	Ensure staff authorized to process data are bound by confidentiality.	**Art. 28(3)(b)**
Security of Processing	Implement appropriate technical and organizational measures.	**Art. 32**
Subprocessor Authorization	May not engage subprocessors without prior written authorization.	**Art. 28(2)**
Assist Controller	Aid controller in ensuring compliance (e.g., DPIAs, rights requests, security).	**Art. 28(3)(f); Art. 35(2)**
Breach Notification	Notify controller of personal data breaches without undue delay.	**Art. 33(2)**
Record-Keeping	Maintain records of all processing activities on behalf of controller.	**Art. 30(2)**
Return or Deletion of Data	Delete or return data upon completion of services.	**Art. 28(3)(g)**
Make Information Available for Audit	Allow controller or auditor inspections for compliance.	**Art. 28(3)(h)**

CCPA/CPRA – Key Duties - Controllers

Duty	Description	CCPA/CPRA Citation
Notice at Collection	Disclose categories and purposes for collection at or before collection.	**§1798.100(b); §1798.110(a)(5)**
Data Minimization & Purpose Limitation	Collect, use, retain only what is “reasonably necessary and proportionate.”	**§1798.100(c)**
Right to Opt-Out / “Do Not Sell or Share”	Provide opt-out for sale or sharing of personal information.	**§1798.120(a); §1798.135(a)**
Right to Limit Use of Sensitive PI	Provide “Limit the Use of My Sensitive Personal Information” mechanism.	**§1798.121(a)**
Consumer Request Response	Provide verifiable processes for access, deletion, correction, and opt-out.	**§1798.130(a); §1798.105–§1798.106**
Nondiscrimination / No Retaliation	Prohibit discrimination or retaliation for exercising rights.	**§1798.125(a)**
Security Obligations	Implement reasonable security procedures and practices.	**§1798.150(a)(1)**
Contractual Obligations	Include required clauses in contracts with service providers, contractors, and third parties.	**§1798.100(d); §1798.140(j), (ag)**
Recordkeeping / Disclosure Metrics	Maintain and publicly disclose metrics if processing large volumes of requests.	**§1798.130(a)(2)**
Training & Compliance Programs	Train individuals handling consumer inquiries or privacy compliance.	**§1798.130(a)(6)**

CCPA/CPRA – Key Duties - Processors

Duty	Description	CCPA/CPRA Citation
Contractual Restrictions	Contract must prohibit selling, retaining, or using PI for other purposes.	§1798.140(j)(1) (Service Provider); §1798.140(ag) (Contractor)
Purpose Limitation	May process data only for business's specified purposes.	§1798.140(j)(1)
No Sale/Share or Cross-Use	Prohibited from combining PI received from multiple sources except for permitted business purposes.	§1798.140(j)(1)(A)–(D)
Security Obligations	Must implement reasonable security measures.	§1798.150(a)(1)
Assistance with Consumer Requests	Assist the business in responding to consumer rights requests.	§1798.140(j)(1)(C); §1798.100(d)(2)
Compliance Verification	Permit the business to monitor compliance (through contractual audit rights).	§1798.100(d)(3)
Certification of Understanding	Must certify compliance with contractual obligations when required.	§1798.100(d)(3)

GDPR; CCPA/CPRA – Data Subject Rights

Right	GDPR	CCPA/CPRA
Access	Obtain copy of personal data and processing details (Art. 15).	Access categories and specific pieces of personal information collected.
Rectification	Correct inaccurate or incomplete data (Art. 16).	Request correction of inaccurate information.
Erasure (Right to be Forgotten)	Delete personal data in certain circumstances (Art. 17).	Delete personal information collected (with exceptions).
Restriction of Processing	Temporarily limit processing (Art. 18).	Not explicitly recognized, though businesses must stop selling/sharing upon opt-out.
Data Portability	Receive data in machine-readable format (Art. 20).	Request data in portable format.
Objection to Processing	Object to processing (including profiling, marketing) (Art. 21).	Opt-out of sale or sharing of personal information.
Automated Decision-Making	Right not to be subject to significant decisions based solely on automated processing (Art. 22).	Right to opt-out of automated decision-making and profiling (added under CPRA).
Information/Transparency	Right to clear, easily accessible information on processing (Arts. 12–14).	Right to notice at collection and transparency about data uses.

GLBA & HIPAA – Sectoral Obligations

GLBA: Privacy notice, opt-out for sharing, safeguards rule

HIPAA: Privacy & Security Rule, PHI protection, breach notification

Implication:

must map overlap of sectoral and general privacy laws

Washington’s My Health My Data Act

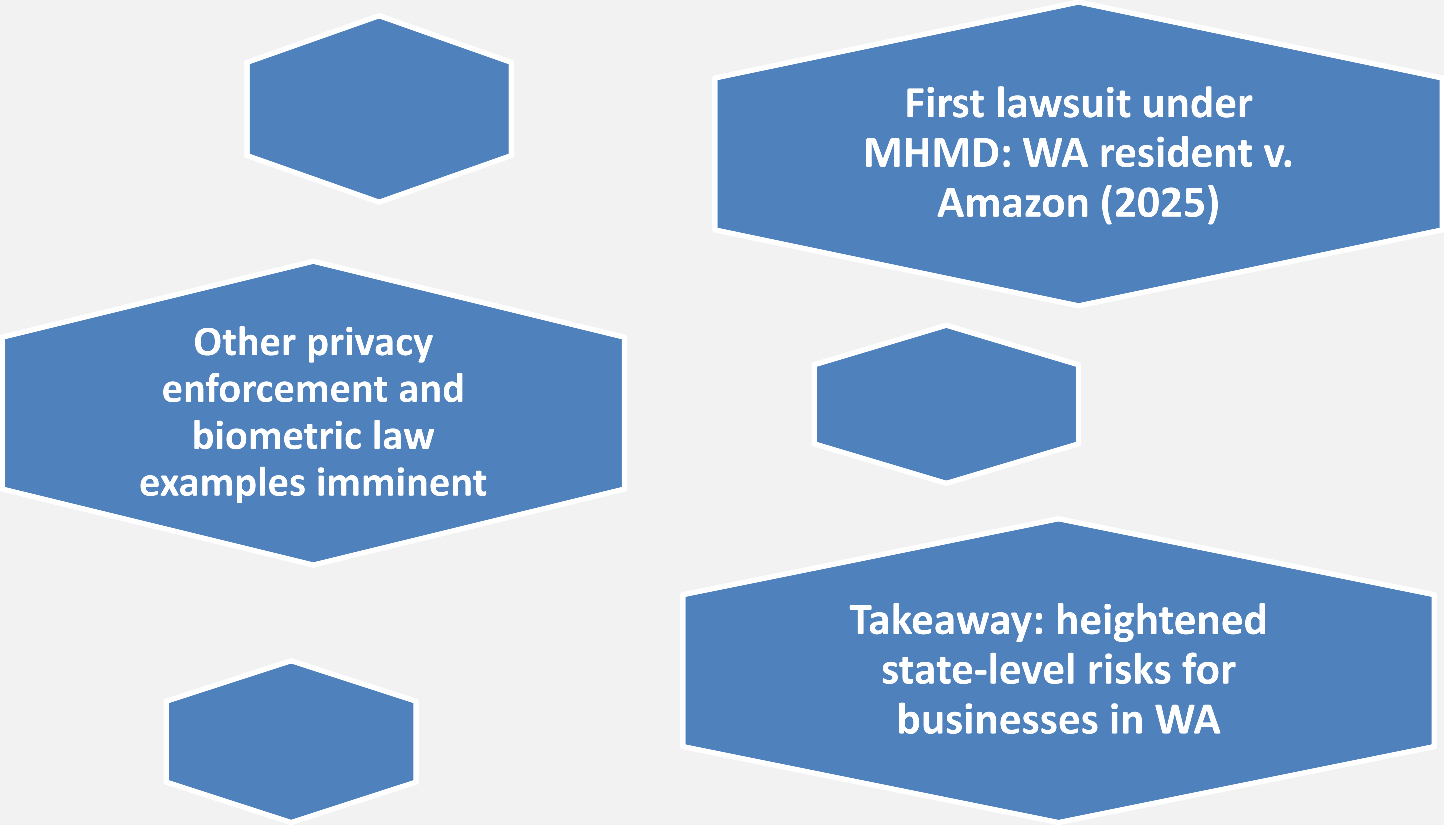
Covers consumer health data not under HIPAA

Consent requirements for (1) collection and (2) sharing

Private right of action under WA Consumer Protection Act

Effective dates: March 31, 2024 (non-small), June 30, 2024 (small)

Case Studies – WA Enforcement

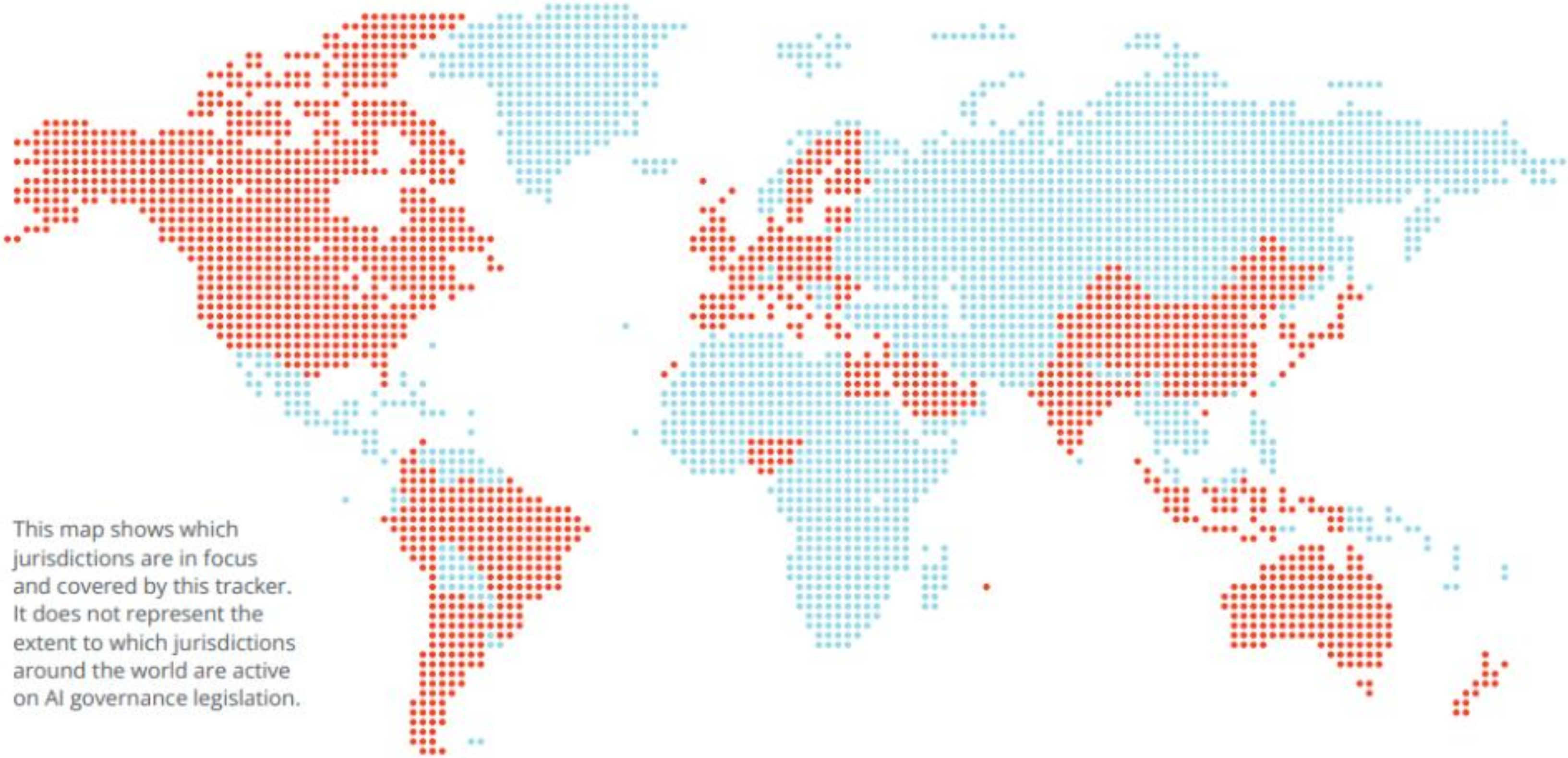


First lawsuit under MHMD: WA resident v. Amazon (2025)

Other privacy enforcement and biometric law examples imminent

Takeaway: heightened state-level risks for businesses in WA

Global AI Law and Policy Tracker



This map shows which jurisdictions are in focus and covered by this tracker. It does not represent the extent to which jurisdictions around the world are active on AI governance legislation.

Jurisdictions in focus

Argentina • Australia • Bangladesh • Brazil • Canada • Chile • China • Colombia • Egypt • EU • India • Indonesia • Israel
Japan • Mauritius • New Zealand • Nigeria • Peru • Saudi Arabia • Singapore • South Korea • Taiwan • United Arab Emirates • U.K. • U.S.

The full resource of the Global AI Law and Policy Tracker is available at: iapp.org/resources/article/global-ai-legislation-tracker/

Why AI Regulation Matters

Rapid growth of AI technologies and risks

Bias

Product Liability

Privacy

Misuse (insurance coverage, financing decisions, automated decisioning),

Deceptive AI marketing claims

Lawyers must assess vendor risk, ethics, regulatory exposure

U.S. AI Regulatory Framework

FTC enforcement under Section 5 FTC Act

Guidance on AI, inquiries into LLMs and chatbots

State AGs investigating AI risk

Regulators apply existing consumer protection & privacy laws;

Additional guidance found under EU AI Act

Case Study – FTC Operation AI Comply

FTC CRACKDOWN ON DECEPTIVE AI CLAIMS (2024)

DONOTPAY SETTLEMENT ($193K) FOR MISLEADING 'AI LAWYER' SERVICE

KEY LESSON:

AI ADOPTION ≠ REGULATORY IMMUNITY

Case Study – Biometric & Chatbot Inquiries

FTC inquiry into companion chatbots marketed to minors (2025)

FTC scrutiny of biometric data practices in AI (2025)

Focus on deceptive practices, bias, consumer protection

Standards & Frameworks

NIST AI Risk Management Framework

IEEE / ISO trustworthy AI standards

Best practices becoming de facto compliance expectations

Why AI Governance?

- It's inevitable that every organization will deploy AI in some form. These pose significant risks without governance
- Ethical duties: competence, confidentiality, supervision
- Governance is the bridge to safe, lawful AI use

Elements of an AI Use Policy

- **Scope**: approved tools, use cases
- **Roles**: approvals, monitoring, auditing
- **Data input controls**: restrict confidential info
- **Vendor oversight**: contracts, audit rights, training data provenance
- **Security controls**: encryption, access, logging
- **Review & incident response plans**

Security & Privacy Controls

- Data minimization & anonymization
- Access controls, encryption
- Vendor contracts with Representations & Warranties, Indemnification, and Audit Rights
- Monitor AI outputs and model drift
- Data lifecycle management

Governance Case Example

FIRM A:

INTERNAL LLM ROLLOUT + RAG STACK + WITH VENDOR CONTRACT + MONITORING

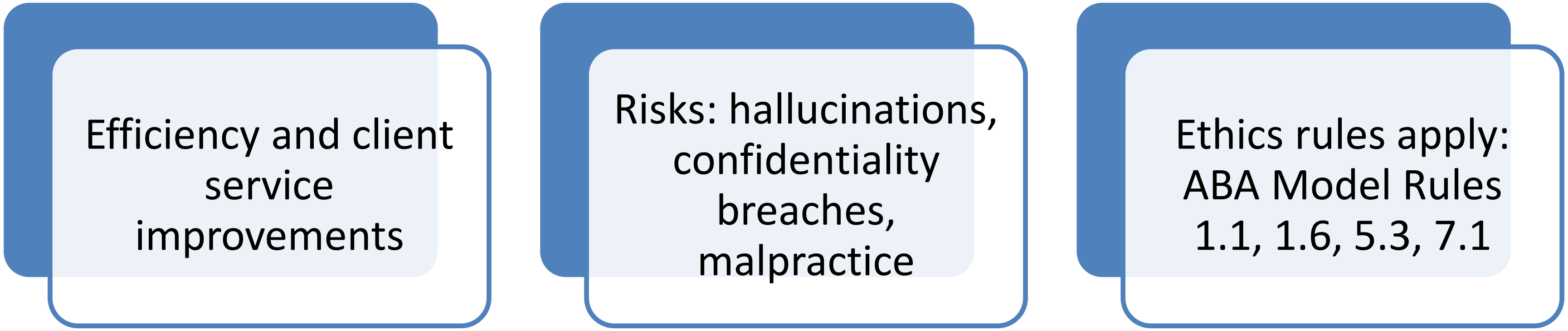
FIRM B:

USED PUBLIC CHATBOT, EXPOSED CLIENT DATA

LESSON:

GOVERNANCE DIFFERENTIATES SAFE FROM UNSAFE ADOPTION

Promise and Pitfalls of AI in Legal Practice



Efficiency and client service improvements

Risks: hallucinations, confidentiality breaches, malpractice

Ethics rules apply: ABA Model Rules 1.1, 1.6, 5.3, 7.1

What is Prompt Engineering?

Designing structured prompts for AI

Influences quality, accuracy, reliability

Legal practice:

drafting, research, review assistance

Certifications and Resources for training and proficiency:

- Clio Legal AI Fundamentals Certification
- Johns Hopkins
- IAPP AI Governance Training

What is Prompt Engineering?

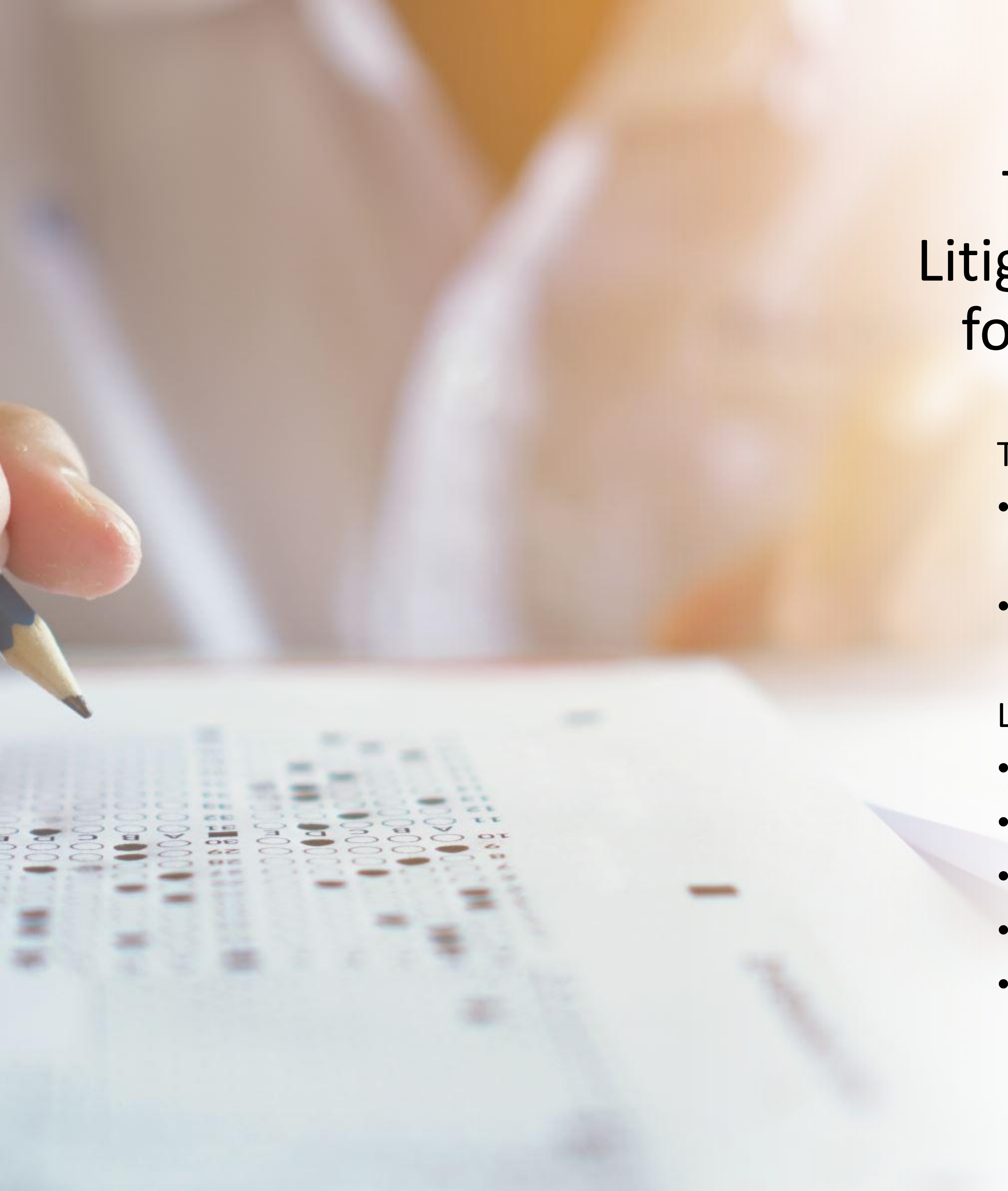
PROMPT: I am drafting a complaint on behalf of [client name]. Give me an argument under Washington State Law that includes case citations as to why the other party that refuses to pay for services is in breach of contract.

RESPONSE: Under Washington law, a party’s refusal to pay for services rendered constitutes a material breach of contract. When one party performs pursuant to an agreement and the other fails to pay, the nonpaying party defeats the essential purpose of the bargain. *See* **Smith v. Evergreen Consulting, Inc.**, 189 Wn. App. 742 (2015) (failure to pay for completed services deemed material breach); *see also* **Johnson v. Cascade Solutions, LLC**, 201 Wn.2d 418 (2020) (payment is a fundamental contractual obligation). Washington courts consistently hold that nonpayment after performance entitles the performing party to damages for breach. *See* **Davis v. Inland Systems**, 172 Wn. App. 553 (2013).

*** From ChatGPT5

Best Practices for Lawyers

- Minimize (or if unsure, eliminate) client data in prompts
- Use templates with guardrails
- **Human review of all AI outputs**
- Maintain prompt + output logs
- Vendor contracts should exclude data training



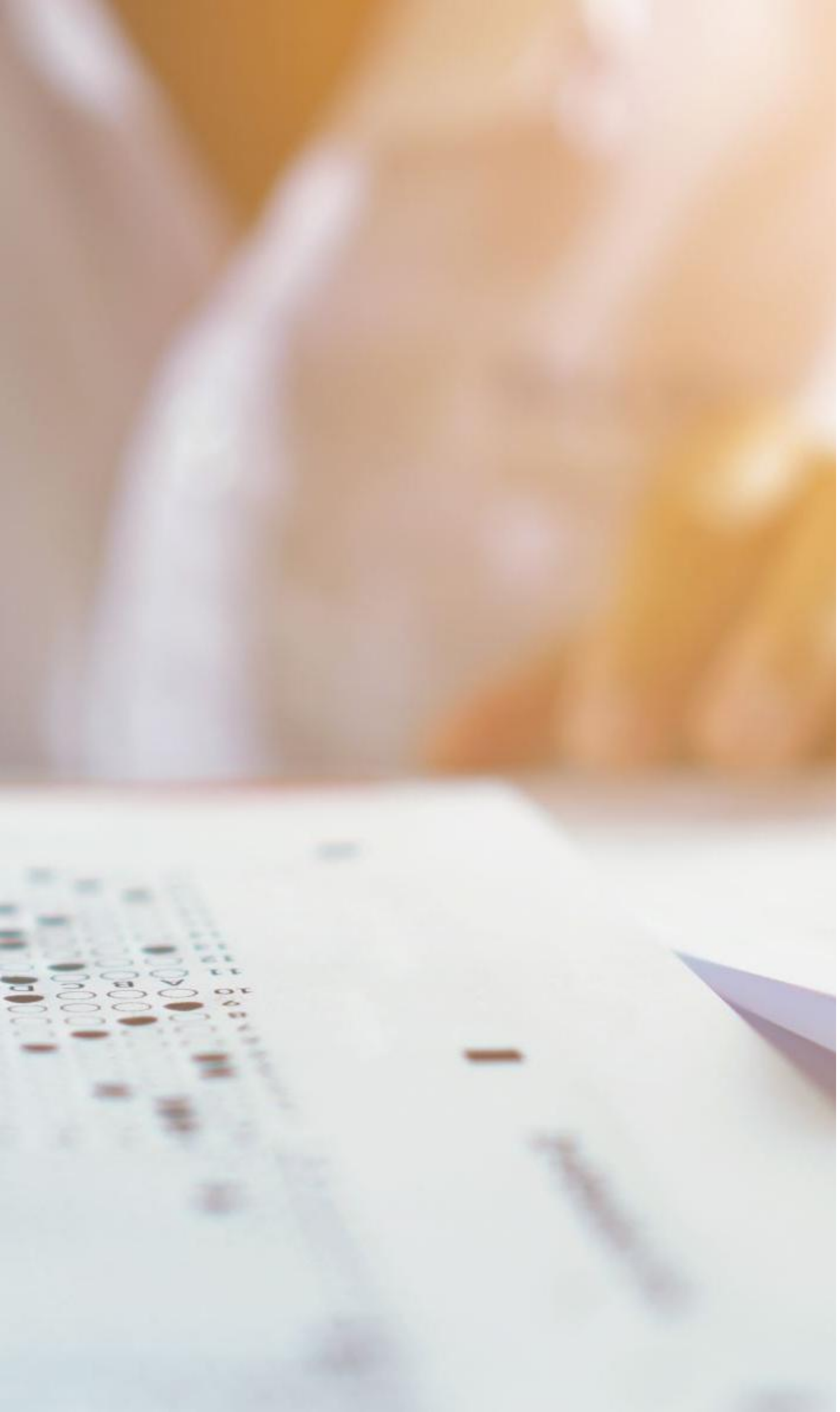
GenAI Transactional and Litigation Solutions built for the legal industry

Transactional and Research

- Drafting, review, due diligence automation
- Legal Research

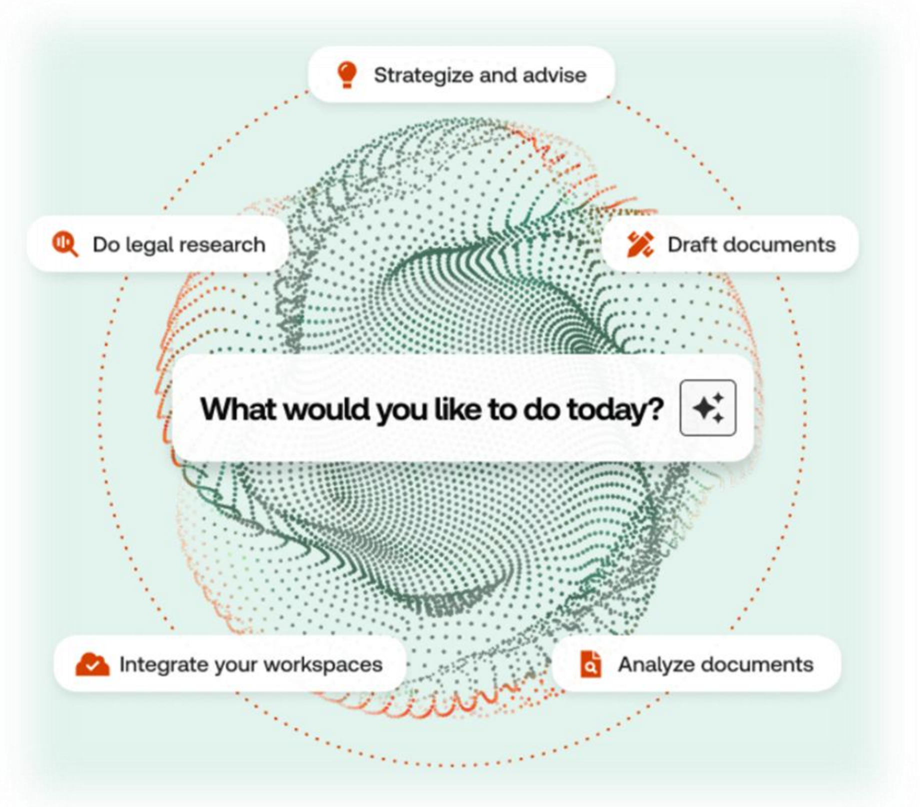
Litigation Support

- Doc Review
- Motion Practice
- Pleadings
- Trial-Prep
- Case Management and Scheduling



Thomson Reuters

CoCounsel



Litmas™

Litmas Eliminates Hallucinations

LITMAS uses a 2-pronged approach to prevent citations to non-existent or irrelevant cases

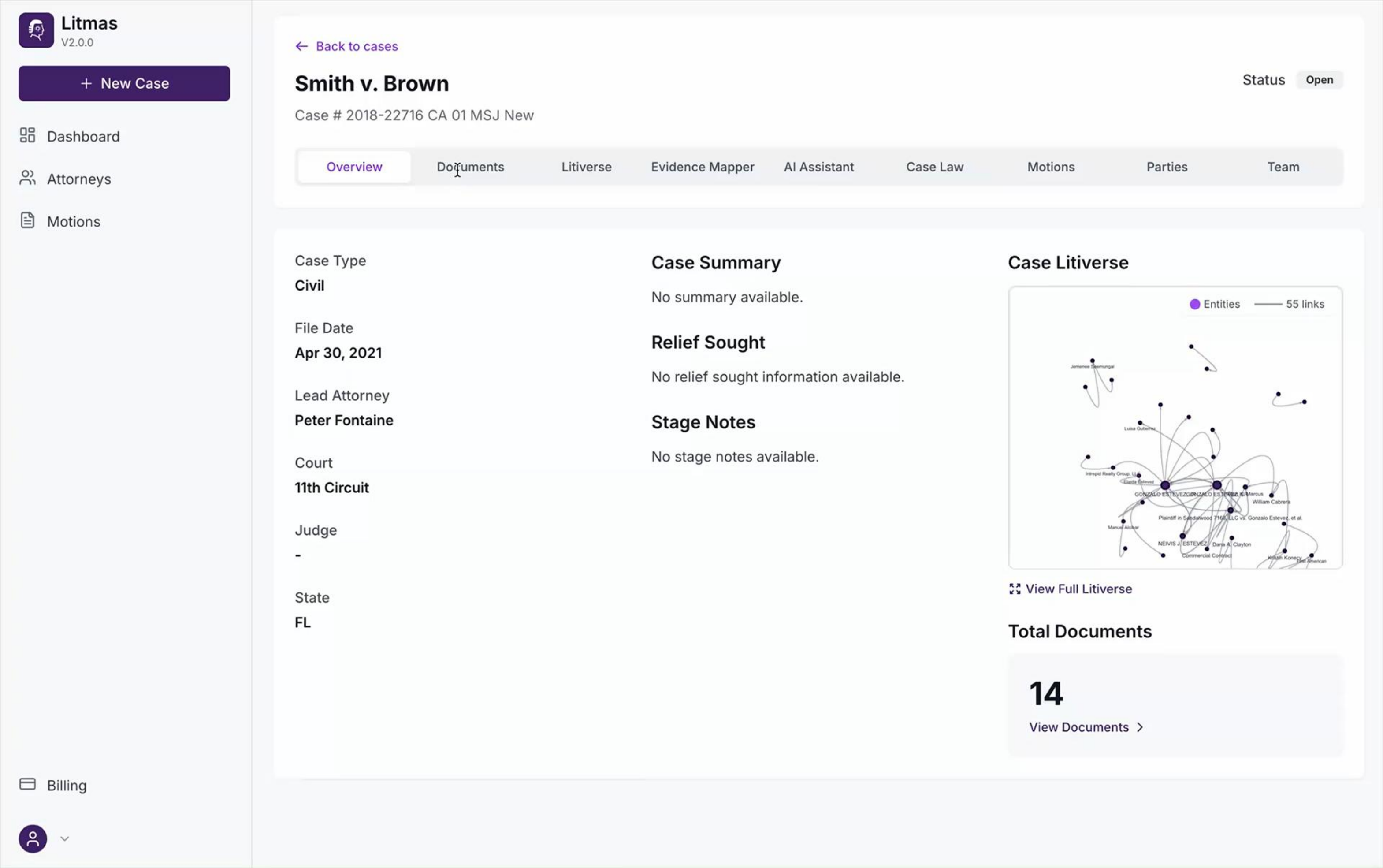
1 Litmas uses the ”RAG” approach meaning the AI is constrained to the universe of facts and caselaw applicable to each case and does not seek answers from outside sources

2 Every case cited by Litmas is verified against a caselaw & statue database and if a case that is cited does not get verified, it is deleted.

100% validated case law and statutes. Real cases. Relevant precedents.

Litigation AI
Built by Litigators

Litmas™



Litmas
V2.0.0

+ New Case

Dashboard

Attorneys

Motions

Billing

← Back to cases

Smith v. Brown

Status **Open**

Case # 2018-22716 CA 01 MSJ New

Overview | Documents | Litiverse | Evidence Mapper | AI Assistant | Case Law | Motions | Parties | Team

Case Type
Civil

File Date
Apr 30, 2021

Lead Attorney
Peter Fontaine

Court
11th Circuit

Judge
-

State
FL

Case Summary

No summary available.

Relief Sought

No relief sought information available.

Stage Notes

No stage notes available.

Case Litiverse

● Entities —— 55 links

View Full Litiverse

Total Documents

14

View Documents >

Implementation Checklist

Vendor due diligence and audit rights

Contract protections: indemnities, liabilities, REPs & Warrants

Internal training, usage policy, human review

Privacy & security controls

Align with ethics duties: confidentiality, supervision

Key Takeaways

Privacy law in the US is a rapidly evolving patchwork (CCPA, GLBA, HIPAA, MHMD)

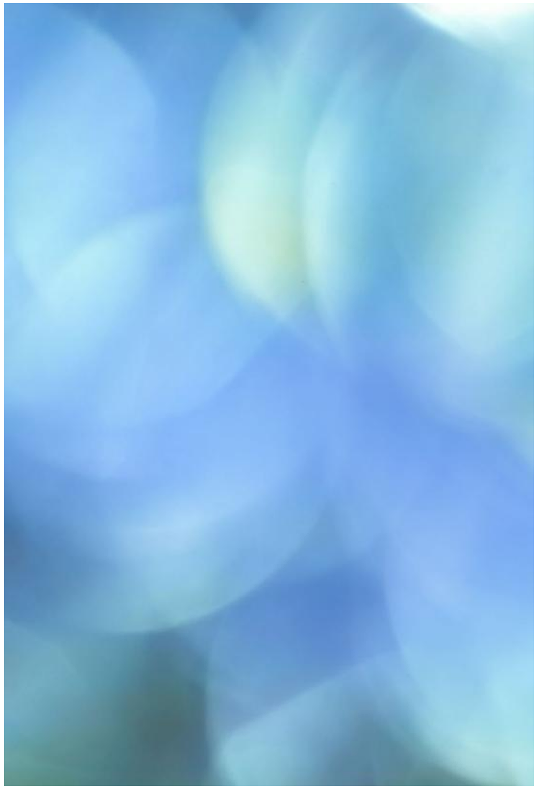
AI regulation enforced via FTC + consumer protection laws

AI governance essential:

policies, oversight, controls

Law firms must balance opportunity with ethical duties

Evaluate enterprise tools with structured checklist



Thank you for attending

Contact:

Gabriel Buehler

Gabriel@buehlerlawpllc.com

509.408.0092

2110 N. Molter Road, Suite 1002

Liberty lake, WA 99019

Citations and References

https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
https://oag.ca.gov/privacy/ccpa https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act https://iapp.org/resources/article/guide-to-the-gramm-leach-bliley-act/ https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true
https://oag.ca.gov/privacy/ccpa
https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act https://iapp.org/resources/article/guide-to-the-gramm-leach-bliley-act/
https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy https://iapp.org/resources/article/washington-my-health-my-data-act-overview/
https://www.orrick.com/en/Insights/2025/02/First-Lawsuit-Filed-Under-Washingtons-My-Health-My-Data-Act
https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes https://www.ftc.gov/ai https://artificialintelligenceact.eu/ https://ai-law-center.orrick.com/us-ai-law-tracker-see-all-states/
https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes https://www.ftc.gov/legal-library/browse/cases-proceedings/donotpay
https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers https://www.hklaw.com/en/insights/publications/2025/06/ftc-evaluating-deceptive-artificial-intelligence-claims https://iapp.org/news/a/consumer-protection-in-the-age-of-ai-the-ftcs-approach-to-ai-regulation
https://www.nist.gov/itl/ai-risk-management-framework https://standards.ieee.org/initiatives/autonomous-intelligence-systems/standards/
https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/ https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/ https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/ https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_7_1_communication_concerning_a_lawyer_s_services/
https://legal.thomsonreuters.com/blog/writing-effective-legal-ai-prompts/ https://libguides.law.gonzaga.edu/c.php?g=1374374&p=10160773