Cookies, Pixels & AI

Managing New Litigation and Regulatory Risks

Peter Stockburger (peter.stockburger@dentons.com)
Brett Dorman (brett.dorman@dentons.com)
Dentons

ACC San Diego
7th Annual MCLE
January 31, 2025

Grow | Protect | Operate | Finance

Cookies, Pixels & SDKs

A growing risk landscape

- **Ubiquitous Tools**. If you have a website or mobile application, you're using them. High risk tooks include adtech and paytech.
- **Regulaory Risk Is Expanding**. State privacy laws impact how these tools can be deployed and used for targeted advertising. Minors complicate the picture. Federal uncertainty remains. Enforcement is on the rise.
- **Litigation Risk Continues To Grow**. A wave of litigation across California and the nation is flooding the courts relating to cookies, pixels, and SDKs. These involve state and federal laws. Real monetary risk.
- **Mitigation Measures Are Available**. Mitigation is not complicated, but it takes work and attention.

Cookies

- A cookie is a small data file stored on an individual's device through their browser.
- Cookies can be set through websites and mobile applications.
- Cookies may be first-party or third-party.
- Third-party cookies present a legal risk if not properly deployed and disclosed.
- Cookies can be blocked by the user.
- Cookies can be session or persistent.
- Cookies can be used for a variety of purposes, including website functionality (e.g., security), remembering preferences, marketing, and advertising.

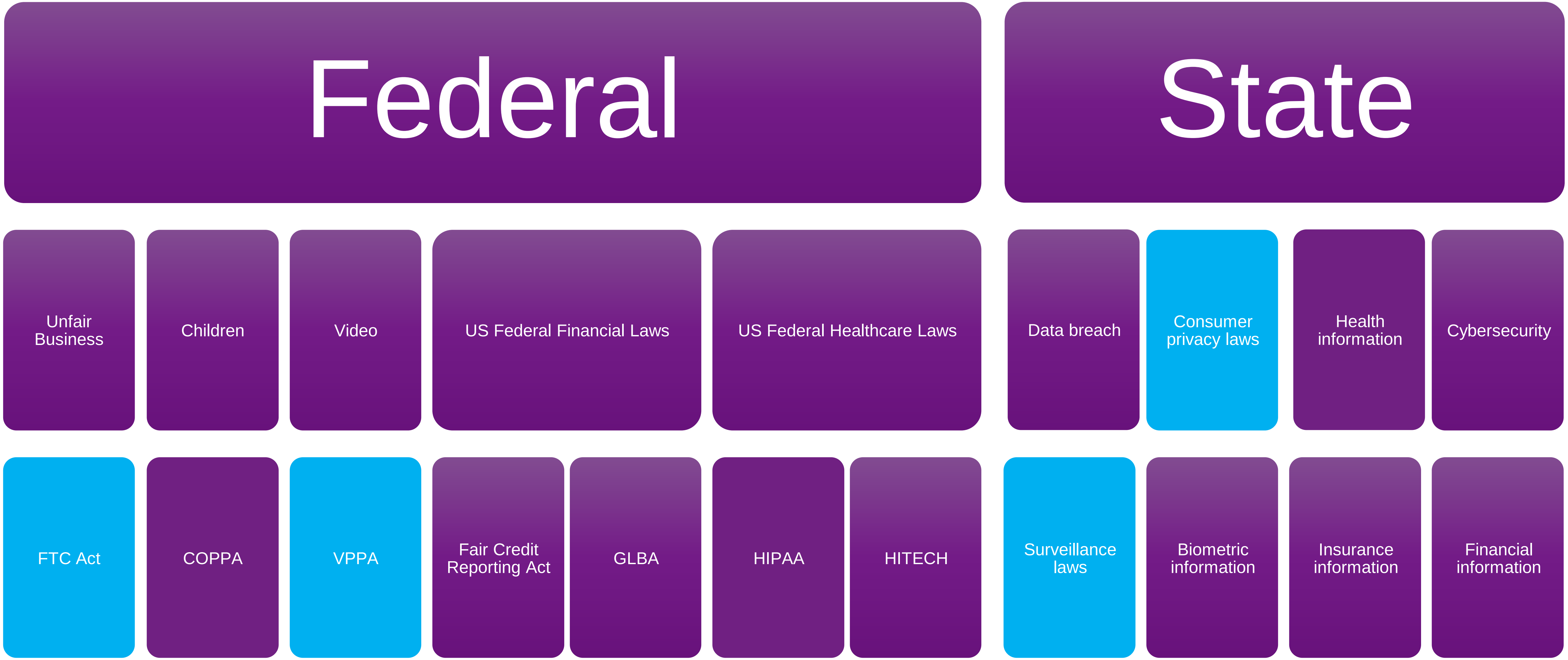
Pixels

- A pixel is a small piece of code that is embedded in a webpage, email, or advertisement to collect information about user behavior / interactions.
- Pixels are always third-party, hosted on third-party servers.
- Pixels are not as easy to detect or block by users, presenting thornier legal issues.
- Pixels are generally used to track conversion rates, performance, and to engage in targeted advertising.
- Meta and TikTok pixels are increasingly the focus of litigants.

SDKs

- SDK stands for a software development kit.
- An SDK is a set of software-building tools for a particular platform, including building blocks, debuggers, and a group of code libraries. SDKs are often used when building mobile applications.
- SDKs can include testing and analytical tools that provide insight into how the application performs in production environments. These may be third-party tools.
- SDKs can be difficult to block through third-party customer tools as their analytics tools are often pervasive and widespread.

US Privacy Landscape



Federal

- Unfair Business
  - FTC Act
- Children
  - COPPA
- Video
  - VPPA
- US Federal Financial Laws
  - Fair Credit Reporting Act
  - GLBA
- US Federal Healthcare Laws
  - HIPAA
  - HITECH

State

- Data breach
- Consumer privacy laws
- Health information
- Cybersecurity
- Surveillance laws
- Biometric information
- Insurance information
- Financial information

Federal Law

FTC Act

- **Increasingly focused** on businesses that use and deploy third-party tracking technologies.
- The FTC historically held companies to account for making false or deceptive promises in their privacy statements relating to the use of tracking technologies.
- In **March 2023**, the FTC issued a blog post that warned organizations using tracking pixels to ensure appropriate disclosures and consents in place.
- FTC is also focused on regulating "**dark patterns**" (i.e., the intentional misleading of a consumer to make a particular choice).
- What will the new administration do?

Federal Law

Video Privacy Protection Act (VPPA)

- **Background**. Passed in 1998 after Bork video rental scandal. Allows a private right of action by a “consumer” against a “video tape service provider” for disclosing video watching history without consent.
- **Key Consideration**. Is your website or mobile application sharing titles or descriptions with third parties?
- **Increased Litigation**. The law was dormant for some time, but recent case law permits consumers to assert a claim even if the underlying service they’re obtaining from your business is not related to video watching.
- **Mitigation Tip**. Consider: (i) minimizing data shared with third parties; (ii) including a link to your terms in your cookie banner; or (iii) obtaining separate consent before videos are watched.

State Law

California Consumer Privacy Act

- **Notice at Collection**. Requires notice at or before the point of collecting personal information, which can include persistent online identifiers.
- **Consent Requirements**. Consent is required if collection and use of personal information goes beyond what a reasonable consumer would expect. How does this impact cookies, pixels, and SDKs?
- **Sale / Sharing**. The use of certain technologies can constitute a “sale” or “sharing” of personal information. Managing consent, tracking opt-outs, and tracking contract provisions becomes critical. GPC signal complicates compliance.
- **Dark Patterns**. Recent regulations make clear that you need parity of choice with the cookie banner, and to avoid dark patterns. What does this mean practically?
- **Mitigation Tip**. Focus on cookie banner, whether consent makes sense, and ensuring SDK’s are picked up.

Enforcement Example

National Retailer

- A large retailer received an investigation notice from the **California AG**, alleging that the opt-out right provided in the mobile application did not fully capture all third-party tracking technologies that may constitute a “sale” under the CCPA.
- An investigation showed that even when a consumer exercised the right to opt-out of the use of third-party tracking technologies, **certain SDKs were still operating** on the mobile application, including for analytics purposes.
- The solution was that the retailer was forced to block certain SDKs when a consumer exercises an opt-out request on the mobile application.
- **Key takeaway**: SDKs can be hard to track!

Enforcement Example

Sephora

- **August 2022**. In the first publicly announced enforcement action, the California AG announced a settlement with **Sephora**.
- AG alleged Sephora failed to disclose to consumers that it was **selling** their personal information, failed to process user requests via a global privacy control, and did not cure these violations.
- Sephora **agreed** to pay $1.2m in penalties and comply with important injunctive terms, including providing mechanisms for users to opt-out.

Enforcement Example

DoorDash

- **February 21, 2024**. California AG announced a settlement with DoorDash under the CCPA and California Online privacy Protection Act (CalOPPPA).
- Allegation was that DoorDash was selling customer personal information **without notice or an opportunity to opt-out**.
- Alleged **DoorDash participated in a marketing cooperative** where businesses contribute personal information of customers in exchange for the opportunity to advertise. CalOPPA allegation put companies on notice.
- **$375,000 penalty plus injunctive relief**, including a duty to provide annual reports to the AG re: ongoing sale or sharing of consumer personal information.

Enforcement Example

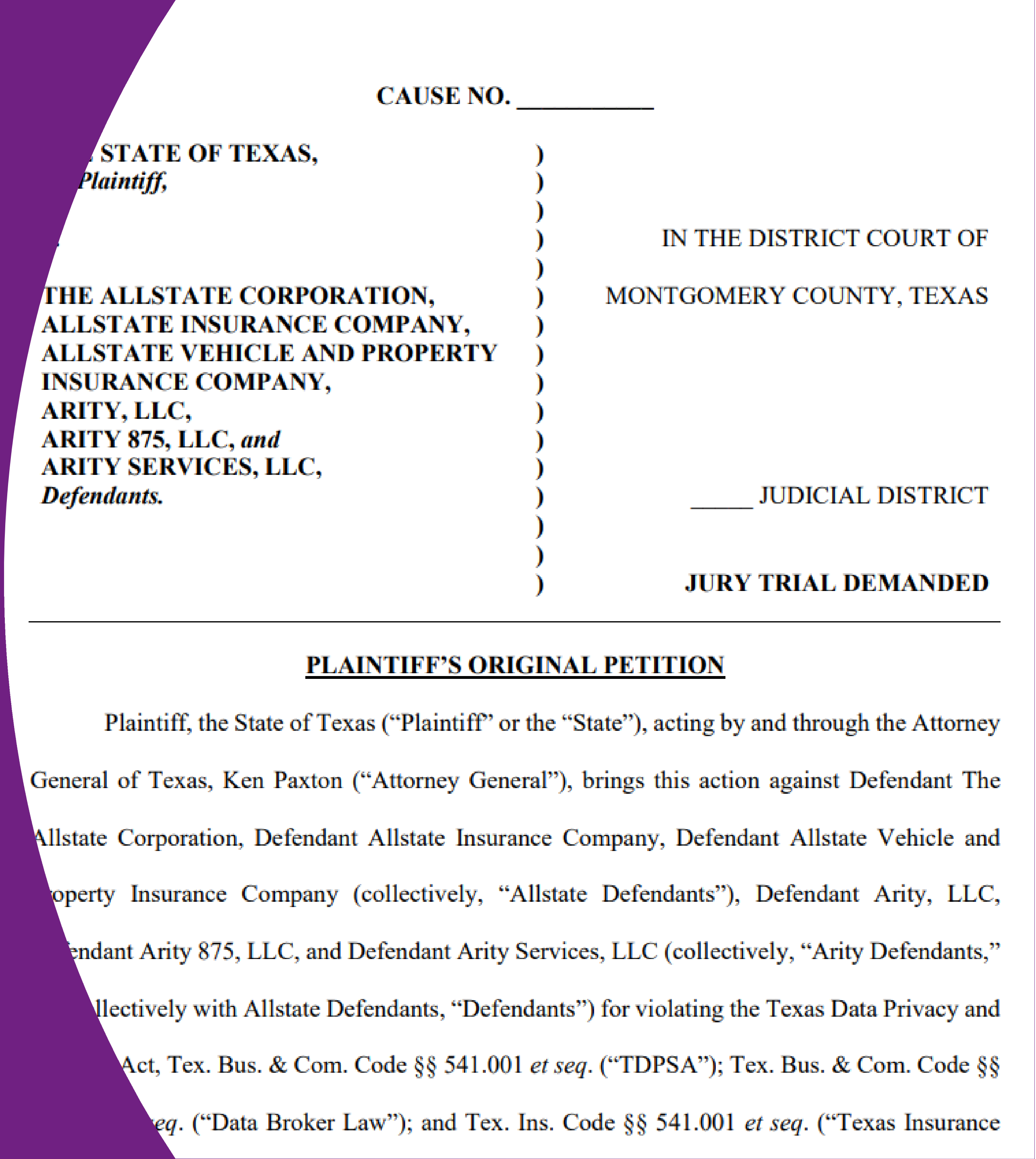
Tilting Point Media

- **July 18, 2024**. Settlement announced by **California AG** and **Los Angeles City Attorney**.
- Alleged Tilting Point Media collected and shared children's data without appropriate consent in violation of the **CCPA** and **COPPA**.
- Specific allegation of **misconfiguring the SDK** leading to children's data being collected.
- Settlement for **$500,000 and injunctive relief** (including implementing and maintaining an SDK governance framework to review the use and configuration of SDKs within its apps).
- **Lesson Learned**: Don't skip the SDKs.

Enforcement Example

Texas - AllState

- **<u>January 13, 2025</u>**. Texas AG filed lawsuit against Allstate and Arity under Texas Data Privacy and Security Act for unlawfully collecting data on over 45 million drivers by deploying tracking software in mobile apps without user consent.
- **<u>Focus on SDKs</u>**. The allegation is that the defendants had an agreement with app developers, and deployed their SDK in exchange for monetary compensation.
- **<u>Key Takeaway</u>**. Regulators are increasingly focused on SDKs and their impact on data collection.



CAUSE NO. __________

STATE OF TEXAS,
Plaintiff,

THE ALLSTATE CORPORATION,
ALLSTATE INSURANCE COMPANY,
ALLSTATE VEHICLE AND PROPERTY
INSURANCE COMPANY,
ARITY, LLC,
ARITY 875, LLC, *and*
ARITY SERVICES, LLC,
Defendants.

IN THE DISTRICT COURT OF

MONTGOMERY COUNTY, TEXAS

_____ JUDICIAL DISTRICT

JURY TRIAL DEMANDED

<u>PLAINTIFF'S ORIGINAL PETITION</u>

Plaintiff, the State of Texas ("Plaintiff" or the "State"), acting by and through the Attorney General of Texas, Ken Paxton ("Attorney General"), brings this action against Defendant The Allstate Corporation, Defendant Allstate Insurance Company, Defendant Allstate Vehicle and operty Insurance Company (collectively, "Allstate Defendants"), Defendant Arity, LLC, endant Arity 875, LLC, and Defendant Arity Services, LLC (collectively, "Arity Defendants," llectively with Allstate Defendants, "Defendants") for violating the Texas Data Privacy and Act, Tex. Bus. & Com. Code §§ 541.001 *et seq*. ("TDPSA"); Tex. Bus. & Com. Code §§ *eq*. ("Data Broker Law"); and Tex. Ins. Code §§ 541.001 *et seq*. ("Texas Insurance

Litigation Risk

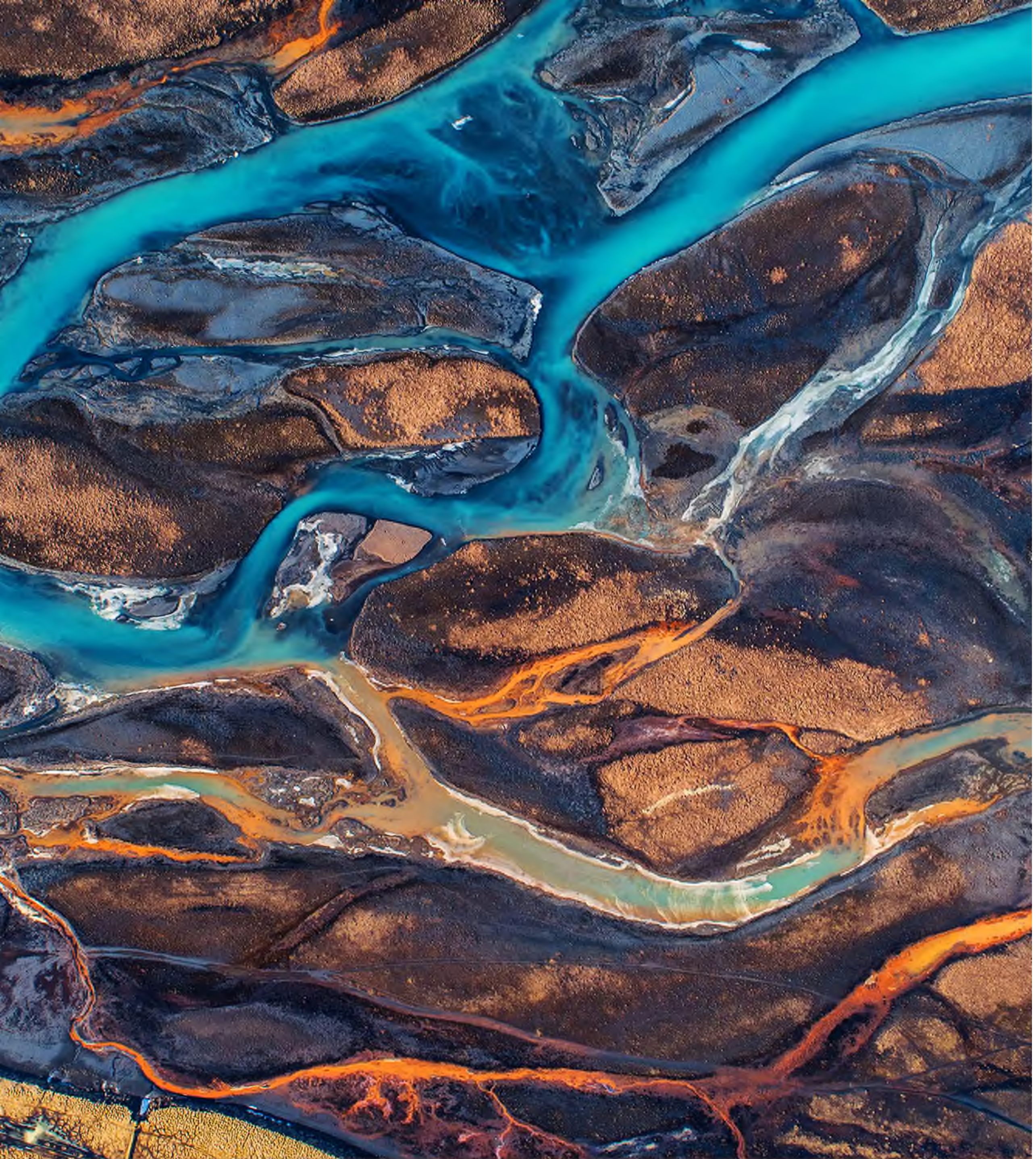
California Invasion of Privacy Act (CIPA)

- **CIPA Scope**. Impacts companies from deploying or “aiding and abetting” the deployment of tracking technologies. Theories range from eavesdropping to pen register.
- **Impacted Use Cases**. Meta pixel, TikTok pixel, chat bots, session replay cookies, SDKs, payment processors.
- **Defenses**. Consent, “service provider” under the CCPA (i.e., party exception), no live “transmission” of the communication due to the nature of the internet.
- **Mitigation strategies**. Enhance cookie banner disclosures, map “service providers” under the CCPA and ensure contract provisions are squared away to eliminate commercialization rights.

Litigation Risk

Song-Beverly Credit Card Act

- **Legal Requirement**. Enacted in 1971, the law prohibits retailers from requesting a consumer's "personal identification information" during or before a credit card transaction. PII is defined as any information that is not set forth on the credit card, such as address and telephone number.
- **Exceptions**. Important exceptions apply, including to verify identity or use for shipping, delivery, or servicing.
- **Lawsuits**. Multiple class action complaints have been filed against name brands, including Patagonia, Vuori, and Lamps Plus.
- **Mitigation Tip**. Use the word "optional" or make clear the information is being used for shipping. Ensure information is not used on the backend for secondary purposes, such as marketing, unless you obtain consent.



Key Takeaways

Third Party Tracking Technologies

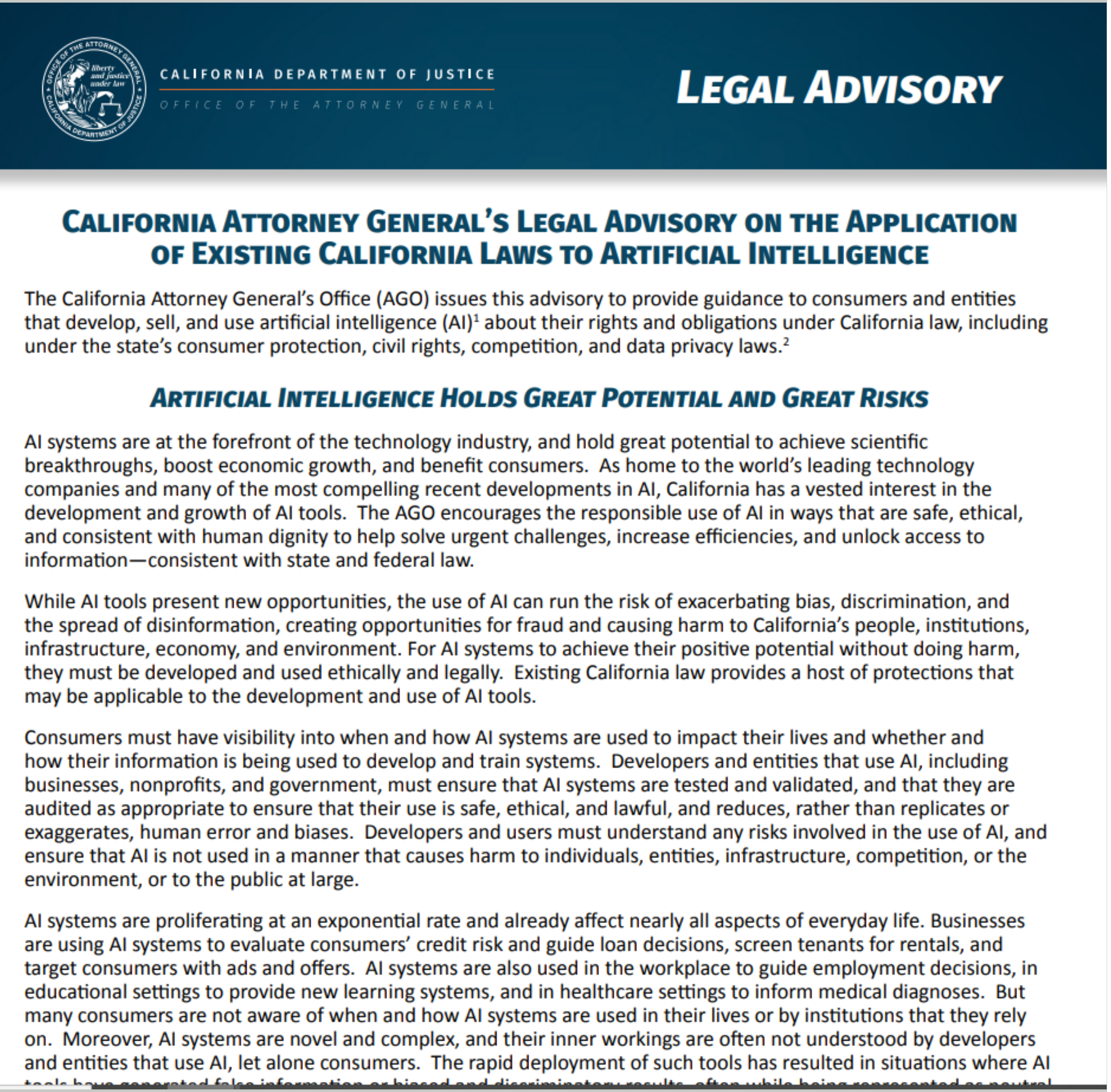
- **Enhance Notice**. Ensure your privacy policy is robust enough to include fulsome disclosures around the use of these technologies. Avoid generalizations.
- **Focus on Cookie Banner Strategy**. The cookie banner is the first line of defense. Consider consent v. notice strategy and impact. Include link to terms to ensure enforceability. Ensure the banner works as advertised.
- **Track SDKs**. SDKs are hard to track, audit, and are generally not captured by the cookie banner / opt-out selections.

AI

Emerging Litigation and Regulatory Risk

California

New AG Guidance



CALIFORNIA DEPARTMENT OF JUSTICE

OFFICE OF THE ATTORNEY GENERAL

LEGAL ADVISORY

California Attorney General's Legal Advisory on the Application of Existing California Laws to Artificial Intelligence

The California Attorney General's Office (AGO) issues this advisory to provide guidance to consumers and entities that develop, sell, and use artificial intelligence (AI)[1] about their rights and obligations under California law, including under the state's consumer protection, civil rights, competition, and data privacy laws.[2]

Artificial Intelligence Holds Great Potential and Great Risks

AI systems are at the forefront of the technology industry, and hold great potential to achieve scientific breakthroughs, boost economic growth, and benefit consumers. As home to the world's leading technology companies and many of the most compelling recent developments in AI, California has a vested interest in the development and growth of AI tools. The AGO encourages the responsible use of AI in ways that are safe, ethical, and consistent with human dignity to help solve urgent challenges, increase efficiencies, and unlock access to information—consistent with state and federal law.

While AI tools present new opportunities, the use of AI can run the risk of exacerbating bias, discrimination, and the spread of disinformation, creating opportunities for fraud and causing harm to California's people, institutions, infrastructure, economy, and environment. For AI systems to achieve their positive potential without doing harm, they must be developed and used ethically and legally. Existing California law provides a host of protections that may be applicable to the development and use of AI tools.

Consumers must have visibility into when and how AI systems are used to impact their lives and whether and how their information is being used to develop and train systems. Developers and entities that use AI, including businesses, nonprofits, and government, must ensure that AI systems are tested and validated, and that they are audited as appropriate to ensure that their use is safe, ethical, and lawful, and reduces, rather than replicates or exaggerates, human error and biases. Developers and users must understand any risks involved in the use of AI, and ensure that AI is not used in a manner that causes harm to individuals, entities, infrastructure, competition, or the environment, or to the public at large.

AI systems are proliferating at an exponential rate and already affect nearly all aspects of everyday life. Businesses are using AI systems to evaluate consumers' credit risk and guide loan decisions, screen tenants for rentals, and target consumers with ads and offers. AI systems are also used in the workplace to guide employment decisions, in educational settings to provide new learning systems, and in healthcare settings to inform medical diagnoses. But many consumers are not aware of when and how AI systems are used in their lives or by institutions that they rely on. Moreover, AI systems are novel and complex, and their inner workings are often not understood by developers and entities that use AI, let alone consumers. The rapid deployment of such tools has resulted in situations where AI tools have generated false information or biased and discriminatory results, often while being represented as neutral

- **Effective Date**. On January 13, the California AG issued two new legal advisories addressing businesses and healthcare related entities.
- **Focus on Existing Authorities**. The AG noted that existing legal authorities impact the development and deployment of AI, including privacy, UCL, and CIPA.
- **Key-Takeaways**. Don't overhype AI in your product, and pay special attention to healthcare deployments. Responsible AI governance approach will help mitigate risk.

CPPA

ADMT Regulations

- **Broad Coverage**. Applies to nearly every type of software. Is triggered when a company is using AI to engage in advertising to consumers.
- **Robust Notice Requirements**. Robust Pre-Use Notice requirement. Requires disclosure of intended use, underlying “logic”, “parameters” used in the model, and other technical and non-technical information.
- **What’s Next?** Open for public comment through end of February. There is a significant appetite to change. Possible limitations on advertising reach as well as definition of applicable AI systems.
- **Can You Prepare Now?** Ensure you’re deploying vendors that have enhanced transparency.

AI Agent Risk

Accountability & Control

- **Increased Autonomy**. AI agents are defined by their autonomy. As autonomy increases in the ecosystem, accountability and control will become larger issues. What will the liability regime be? Who is contractually responsible?
- **API Access Becomes Critical**. AI agents need access to tools to complete tasks. What tools are they permissioned? How do you control highly restrictive API calls, and how is that being documented? How dialed in is security and IT?
- **Generative AI Agents & Accuracy**. As AI Agents are making representations to individuals, who is accountable? How can accuracy be ensured (i.e., human-in-the-loop) when the purpose of an AI Agent is to take the human out of the loop?

Utah

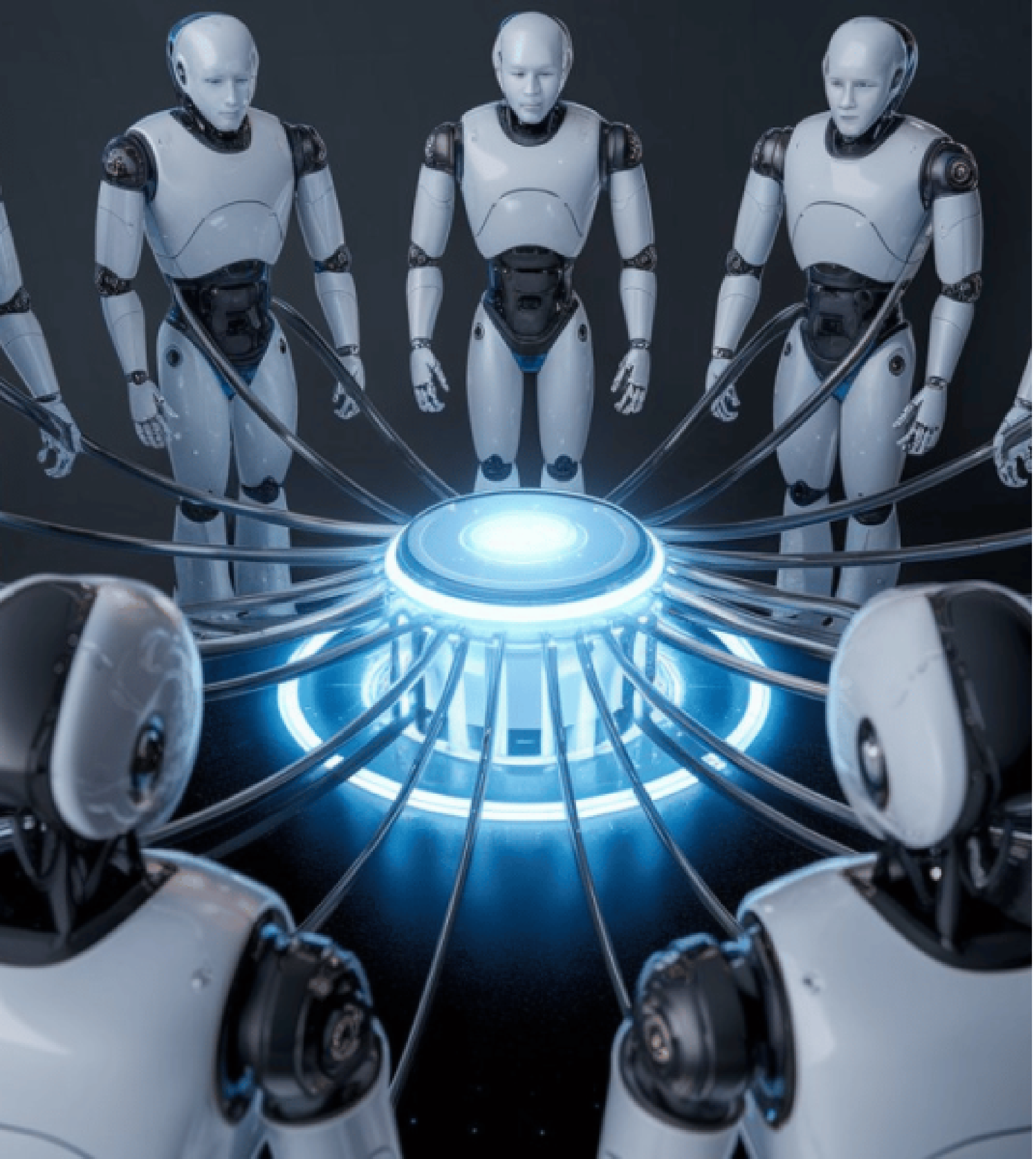
Artificial Intelligence Policy Act

- **Effective Date**. May 1, 2024
- **Application**. Applies to the use of generative AI.
- **General Requirements**. For general organizations, must disclose to a consumer if generative AI is being used if asked.
- **Regulated Professional Requirements**. Regulated professionals (i.e., health care) must disclose verbally or in writing prior to using generative AI.
- **Enforcement**. No private right of action. Enforced by Utah Division of Consumer Protection and Attorney General. $2,500 - $5,000 per violation.
- **Defense**. No defense to blame AI for consumer protection violations.

Colorado

New AI Law

- **Effective Date**. February 1, 2026
- **Passed**: May 17, 2024
- **Scope**. Imposes governance, risk assessments, disclosure, and documentation requirements on developers and deployers of AI. Impacts “high-risk” AI systems, which can relate to the delivery of health care.
- **AI System**. Any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.
- **Governor Statement**. Hopes the law to receive some clarity before 2026 effective date so scope may change.
- **Enforcement**. No private right of action.



Mitigating AI Risk

Responsible AI Governance

- **Be Responsible**. Regulators, stakeholders, and law makers across the globe are looking for deployers of AI (including AI agents) to do so “responsibly” and in alignment with leading AI governance frameworks. Vet your vendors. Due your diligence. Formulate your policy and strategy.
- **Focus on accountability and permissions**. As more advanced AI becomes available, ensure the appropriate teams have built in accountability / review processes that are explainable and reasonable. Ensure data permissions, API permissions, and other technical controls are thought through.
- **Track Public Statements and Litigation Risk**. Public facing AI presents a significant risk. Ensure uses are aligned with emerging legal standards.
- **Educate your workforce**. IT, marketing, legal, and HR may be presented with opportunities. Educate on the technology. AI literacy is critical.

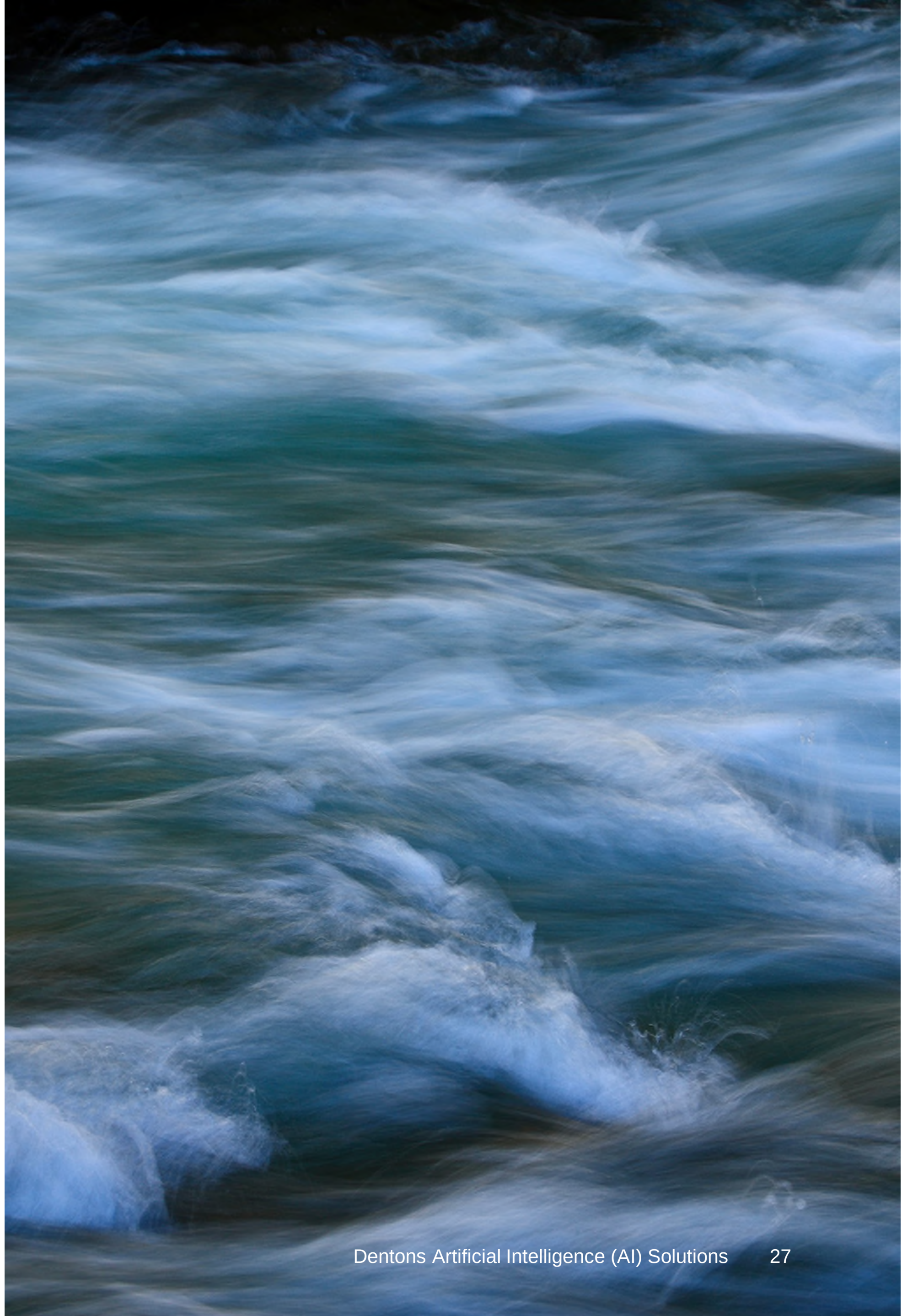
Appendix

Dentons Capabilities

Dentons
Artificial Intelligence (AI) Solutions

Why choose Dentons for AI?

	Benefits to you
Global footprint 75+ partners in 80+ jurisdictions have AI expertise. Many of our team have worked together countless times on multijurisdictional projects.	- Best of local and global - Global knowledge at fingertips - Global regulatory insight - Team ready to mobilize
Innovation is in our DNA Dentons is a firm of firsts, including one of the first to invest in, and promote legal tech via, Nextlaw Labs. We have a team of innovators across our markets that procure and develop AI solutions.	- Clients benefit from Dentons own experience with AI and innovation - Team adept at understanding the procurement, development and application of AI across different business functions
Deep expertise Our full-service AI team provides cross-discipline solutions to help you successfully develop or deploy AI technologies.	- Joined-up solutions and thinking, whether you need support with governance, agentic development, data privacy, procurement, IP, employment, disputes or M&A
Track record Our credentials, reputation and client base in the AI space are outstanding and include being appointed as legal advisor to the Artificial Intelligence Safety Institute.	- We are not learning on the job - We are experienced advisors in the AI space - Trusted market leaders
Added value As market and thought leaders, we produce knowledge, webinars and guidance.	- Insights, knowledge hubs, webinars and crisis simulation experiences – available to you at no charge



Supporting your AI journey

Artificial Intelligence (AI) is a transformative force, presenting challenges and opportunities for all organizations across all sectors. We partner with clients across the AI development and deployment journey.

Our full-service global AI team provides solutions to help you successfully develop and deploy AI technologies to support your organization’s strategy, while navigating the complexity of existing and future regulations.

With 75+ partners and fee earners advising in 80+ jurisdictions worldwide, our global AI team provides market-leading legal advice around the world. Our team comprises leading AI experts advising across all key areas, including:

- **AI governance**
- **Data privacy and cybersecurity**
- **AI projects and procurement**
- **Employment and talent management**
- **IP protection and enforcement**
- **Disputes and managing liability**
- **M&A and investments**

Supporting your AI journey

“The Dentons team were quick to wade into the AI space and delivered some high-quality training sessions early on. They have guided us on our internal generative AI strategy, including advising on key risks and mitigations, the regulatory landscape, onboarding AI suppliers and our internal strategy and guidelines. They have demonstrated deep knowledge of available generative AI tools and have made pragmatic suggestions for how to mitigate risk whilst continuing to explore this space.”

Legal 500 2025 – Artificial Intelligence

Visit Dentons’ AI: Global Solutions Hub which provides in-depth insights into the opportunities and challenges AI presents, the essential legal issues to consider, practical recommendations to navigate AI transformation and information on key trends at all stages of AI development.

16:04 Fri 16 Aug
AA
DENTONS
Global sectors
Global solutions
Client experience
Our people
AI: Global Solutions Hub
Grow
Protect
Operate
Finance
Latest CX webinar: Key trends in AI governance, procurement and deployment
October 2024
Webinar recording: Key trends in AI governance, procurement and deployment
CX Webinar Program
Download our global AI regulatory landscape overview
Global regulatory landscape: an overview

Dentons US Core Team

Peter Stockburger (Inuit Lead)

Partner | San Diego

US AI Advisory Team Lead

Peter leads the US AI Advisory team, is a member of the firm's Global Venture Technology and Emerging Growth Companies group, and co-leads the firm's Global Autonomous Vehicles Practice. Peter's partners with clients around the globe to help them develop smart data and product strategies, design and deploy AI responsibly, ensure compliance with an increasingly complex data privacy legal landscape, and ensure cybersecurity policies practices are leading edge. Peter is a recognized expert on AI governance, having spoken to lawmakers at the federal and state level on the future of AI global governance. Peter is also a frequent author and speaker on all things AI, privacy, and cybersecurity.

Brett Dorman

Managing Associate | Los Angeles

Brett is a member of the firm's Global Venture Technology and Emerging Growth Companies group and the US AI Advisory Team. Brett's practice focuses on technology transactions and data privacy and cybersecurity, spanning a wide range of industry sectors and emerging technology subject matter including, fintech, healthtech, adtech, blockchain technologies (including cryptocurrency and NFTs), big data and AI. He assists clients with day-to-day contracts for technology and commercial transactions, data privacy and cybersecurity compliance, AI governance, and the deployment of new technologies.

Natalie Hoeper

Counsel | New York

US AI Advisory Team Co-Lead

Natalie co-leads the US AI Advisory Team, and is a member of the firm's Global Venture Technology and Emerging Growth Companies group. Natalie advises clients ranging from early-stage startups to large-scale international corporations, including working with everyone from friends-and-family round entrepreneurs to some of the largest global brands in the world. Natalie represents clients in a range of sectors on commercial transactions, data privacy and intellectual property. She assists clients on commercial contracts, technology, licensing, and content distribution agreements in the fields of AI, amongst other emerging technologies.

Anthony Anderson

Managing Associate | Silicon Valley

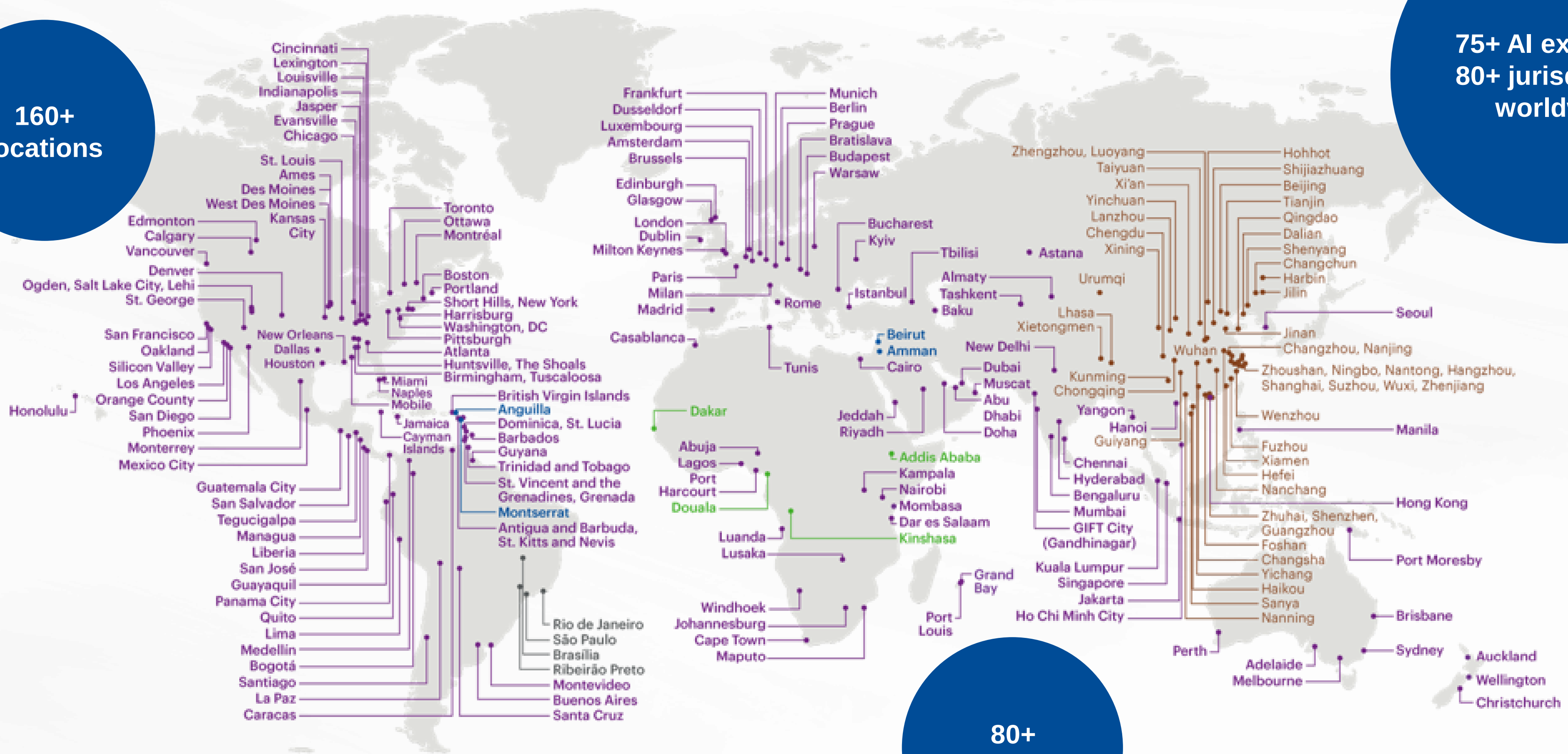
Anthony is a member of the firm's Global Venture Technology and Emerging Growth Companies group and the US AI Advisory Team. Anthony assists clients with navigating the complex intersection of AI, data privacy and cybersecurity. Based in both Silicon Valley, CA, and Washington, DC, Anthony Anderson bridges the epicenter of tech innovation with the heart of policymaking, giving him an unparalleled edge in advising clients at the intersection of AI, data privacy and cybersecurity. Anthony Anderson's expertise lies in "next-generation technologies"—a thematic grouping of AI, data privacy and cybersecurity that reflects how these areas shape our digital future. Anthony has prior experience working both in-house with an autonomous vehicles company and in the White House for President Biden.

Unrivalled global reach

160+ locations

75+ AI experts in 80+ jurisdictions worldwide

80+ countries



Locations in purple represent Dentons offices.

Locations in blue represent associate firms, offices, jurisdictions of practice from other Dentons' offices or special alliances as required by law or regulation.

Locations in green represent approved associations that have not yet been formalized.

Locations in gray represent Brazil Strategic Alliance.

大成 is Dentons' preferred law firm in China.

ABOUT DENTONS

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you.

www.dentons.com