

Client Alert

Special Matters & Government Investigations

MAY 20, 2025

For more information, contact:

Nema Milaninia
+1 202 626 9273
nmilaninia@kslaw.com

Alicia C. O'Brien
+1 202 626 5548
aobrien@kslaw.com

Eve-Christie Vermynck
+44 20 3929 5335
evermynck@kslaw.com

Charly Helleputte
+32 2 898 0237
chelleputte@kslaw.com

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

King & Spalding

London
8 Bishopsgate London
EC2N 4BQ
United Kingdom
T. +44 20 7551 7500

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
T. +1 202 737 0500

Brussels
Bastion Tower
5 Place du Champ de Mars
1050 Brussels
Belgium
T. +32 2 898 0200

Transatlantic AI Governance – Strategic Implications for U.S. — EU Compliance

INTRODUCTION: THE GLOBAL RACE TOWARDS AI GOVERNANCE TAKES DIFFERENT PATHS

As artificial intelligence (AI) continues to transform global markets, the European Union and the United States are advancing regulatory frameworks that reflect starkly different legal traditions, political priorities, and economic strategies. These are often framed as competing visions—regulation versus innovation—but in practice, the divide is more complex. What has emerged is not just divergence, but rising tension and growing misalignment across transatlantic AI governance.

This regulatory tension is shaped as much by geopolitics as by policy. Questions of economic competitiveness, digital sovereignty, and values-based governance are now embedded in legal and institutional debates over AI oversight. For companies operating across both jurisdictions, the result is a fragmented and increasingly unpredictable compliance environment.

This client alert unpacks that environment in three parts:

- Part I maps the key legal distinctions between the EU and U.S. approaches;
- Part II explores the strategic and political tensions these differences have triggered, both bilaterally and in global governance forums;
- Part III offers actionable strategies for navigating overlapping regulatory demands, anticipating enforcement trends, and aligning compliance with broader operational and market-entry goals.

The bottom line: AI compliance is no longer just a legal obligation. It is a strategic imperative—one that requires a forward-looking, risk-calibrated approach rooted in jurisdictional awareness, regulatory engagement, and organizational readiness.

PART I: CONTRASTING REGULATORY FRAMEWORKS

While often portrayed as a stark contrast between regulation and innovation, the divide between the EU and U.S. approaches to AI governance is more nuanced.

The EU has enacted the first binding, cross-sectoral legal framework for AI through the [EU Artificial Intelligence Act](#) (EU AI Act), emphasizing transparency, risk mitigation, and regulatory supervision (see [EU & UK AI Round-Up](#)). At the same time, EU policymakers continue to promote a pro-innovation agenda, highlighting sandboxes, funding mechanisms, and industrial strategy—though many question whether these initiatives can offset the compliance burdens created by the EU AI Act.

In the U.S., the current legal landscape remains fragmented and sector-specific, but federal policy has largely leaned toward enabling innovation through flexible, non-binding guidance. Without a unified legal framework, U.S. AI governance tends to be more fragmented and reactive – particularly at the state level where over 500 AI bills have been proposed in Q1 of 2025 alone (for more see [AI Quarterly Update](#)). That orientation may shift, however, as the administration considers new executive actions and as Congress appears to be interested in resolving regulatory conflicts at the state level.

For companies operating in both jurisdictions, what appears to be a binary choice between regulation and innovation is converging into a more complex policy environment:

- 1. Legal Scope and Structure:** The EU AI Act is a comprehensive legal framework governing the development, placement on the market, and use of AI systems. It applies across sectors, with obligations based on risk categorization. In contrast, the United States continues to follow a sector-specific approach rooted in existing statutory authorities and agency mandates. There is no standalone federal AI law, and legislative momentum for such a framework remains limited. That said, President Trump is expected to announce his AI Action Plan in July 2025, which could lay the groundwork for new executive orders or federal efforts to reshape AI oversight.
- 2. Risk Classification and Compliance Requirements:** The EU AI Act divides AI systems into four risk levels: unacceptable, high, limited, and minimal. Unacceptable systems, like those that manipulate or exploit users, are banned. High-risk systems—such as those used in biometrics, hiring, or critical infrastructure—must meet strict requirements, including risk assessments, human oversight, technical documentation, and EU registration. General-purpose AI (GPAI) models that could cause systemic risk face extra rules, especially if widely used in the EU (e.g., over 10,000 business users). In contrast, the U.S. has no formal risk-tiering system. Oversight is reactive and case-by-case, conducted by agencies such as the Federal Trade Commission (FTC) and Department of Justice (DOJ) under existing consumer protection, civil rights, and competition laws. State laws add further complexity, often with varying and conflicting compliance mandates.
- 3. Governance and Enforcement:** The EU has set up a full enforcement system for the AI Act that includes: (1) the EU AI Office to oversee enforcement and issue guidance; (2) the EU AI Board to help apply the EU AI Act consistently; (3) an expert group to provide technical advice; and (4) the appointment by each Member State of at least one notifying authority and one market surveillance authority (together called national competent authorities) to enforce the respect for fundamental rights in relation to high-risk AI systems, and oversee independent assessors. In contrast, U.S. enforcement is led by federal agencies operating under legacy laws, without a central AI regulator. For instance, the FTC has taken the lead on AI investigations, but its tools remain limited. States have filled the gap, producing inconsistent enforcement priorities across jurisdictions.
- 4. Extraterritorial Reach:** The EU AI Act applies to any provider or deployer placing AI systems on the EU market or whose outputs are used in the EU—regardless of the company's location. Non-EU providers must appoint a local

representative and comply with applicable obligations. By contrast, U.S. AI regulation generally lacks extraterritorial scope.

- 5. Transparency and Disclosure Requirements:** Under the EU AI Act, providers of high-risk systems must disclose AI use, maintain explainability, log performance, and provide summaries of training data for generative systems. In contrast, the U.S. imposes no comparable general transparency requirement; disclosures are typically voluntary or guided by sector-specific regulations.
- 6. Treatment of General-Purpose AI (GPAI):** The EU has introduced detailed GPAI obligations—including documentation, risk mitigation, and security measures—with codes of practice in development. The U.S. does not yet distinguish GPAI in law.
- 7. Regulatory Sandboxes and Innovation Support:** The EU AI Act mandates that Member States establish regulatory sandboxes to support supervised testing and legal certainty for new AI technologies. While the U.S. has innovation hubs within federal agencies and issues informal guidance (e.g., FTC staff opinions), it lacks a comparable national sandbox framework.
- 8. Penalties and Liability Exposure:** EU penalties for violations of the EU AI Act can reach the higher of €35 million and 7% of global annual turnover for the preceding financial year. These fines are intended to be dissuasive and apply to a wide range of breaches. In contrast, the U.S. does not impose AI-specific fines of this magnitude. Enforcement is generally governed by existing statutes with lower and more varied penalty ceilings.

In view of these legal divisions, companies will need to implement legal and compliance strategies that bear in mind the following considerations:

Market Entry Considerations. For companies developing general-purpose or high-risk AI systems, the regulatory burden of complying with the EU AI Act can be significant. As a result, a core strategic question is whether to launch products in the EU at all—or to structure deployment, marketing, and distribution models in ways that avoid triggering jurisdictional reach. For some, bypassing the EU market altogether may be a rational trade-off to preserve product agility and reduce compliance overhead in the early stages of deployment.

Non-compliance carries significant liability exposure. While the draft GPAI Code of Practice is formally voluntary, failure to adopt it may carry adverse legal and regulatory consequences. Under the current proposal, non-adoption could trigger a reversal of the burden of proof, effectively requiring companies to demonstrate compliance with applicable safety, transparency, and governance obligations in the event of enforcement or litigation. This would elevate the GPAI Code of Practice (once finalized) from a best-practice guideline to a baseline standard for demonstrating responsible AI development and deployment—particularly for providers of general-purpose AI models.

Companies also face requalification risk—deployers or importers may be deemed “providers” if they significantly alter the AI system or repurpose it for high-risk use, thereby inheriting full regulatory obligations.

Managing the U.S. Patchwork. The absence of a unified federal AI law in the U.S. leaves companies exposed to a patchwork of federal and state rules. Sector-specific oversight from the FTC and others have been complemented by state compliance strategies—especially as states advance laws on algorithmic transparency, bias, and automated decision-making.

Additionally, companies contracting with the U.S. government must comply with specific acquisition rules under OMB Memorandum M-25-21, including for high-impact AI, risk management protocols, data rights, and vendor lock-in protections.

Overlap with Non-AI-Specific Laws. Both the EU and U.S. regulate AI through preexisting frameworks. AI systems often implicate GDPR, HIPAA, intellectual property laws, anti-trust laws, financial regulations, and product liability regimes. Ensuring compliance across these overlapping domains requires coordination between a cross-functional AI governance structure, which should at least include representatives from the legal, compliance, and technical teams.

PART II: SPECIFIC POINTS OF TENSION IN TRANSATLANTIC AI REGULATION

While Part I outlined the structural and legal differences between the EU and U.S. approaches to AI regulation, recent developments have turned these differences into concrete points of friction. What began as diverging regulatory models has become a broader contest over how AI should be governed—raising legal, political, and strategic tensions that now extend beyond domestic policy.

These tensions are increasingly visible on the international stage. Efforts to coordinate global AI governance—through forums like the Bletchley Declaration (UK, 2023), the Seoul AI Summit (May 2024), and the Paris AI Action Summit (February 2025)—have led to high-level agreement on general safety principles, but major gaps remain. At the Paris summit, for instance, the U.S. declined to join the EU-backed “Inclusive and Sustainable AI” declaration, underscoring its skepticism toward EU-style regulation. The drafting of the Council of Europe’s AI Treaty also highlighted these divides, with both sides seeking influence but neither securing alignment.

Together, these events reflect how the EU-U.S. division on AI is evolving into a global competition to shape the rules, values, and market structures that will define the next generation of technology.

1. Innovation vs. Regulation: Competing Economic Models: The Trump administration has emphasized deregulation and economic sovereignty as pillars of U.S. leadership in AI. A January 2025 Executive Order entitled “Removing Barriers to American Leadership in Artificial Intelligence” instructed agencies to reduce regulatory burdens and promote “ideological neutrality” and “market performance” in AI development and called for eliminating barriers to ensure the U.S. remains the “unrivaled world leader” in AI. Michael Kratsios, Science and Technology Advisor to President Trump, also has emphasized a vision where the U.S. government acts as both promoter and early adopter of American AI technologies.

EU leaders have sought a legal framework that is intended to be balanced, risk-based and promotes trust rather than stifling growth. European Commission Executive Vice Presidents Teresa Ribera and Henna Virkkunen have stressed that EU rules apply equally to all actors—whether American, Chinese, or European. The recent withdrawal of the proposed AI Liability Directive, according to Commissioner Virkkunen, reflects the EU’s commitment to encouraging innovation while maintaining accountability. Furthermore, the EU AI Office recently published its AI Continent Action Plan reiterating that while it is committed to regulating AI, it also intends to assist with compliance and foster AI innovation to turn the EU into a leading “AI continent,” including a continuous focus on investing in supercomputer infrastructure expected to reach €10 billion by 2027 by launching AI Gigafactories alongside existing AI factories.

2. Allegations of Targeting U.S. Firms: President Trump has referred to EU fines as a “form of taxation” on U.S. companies. Vice President J.D. Vance has criticized “foreign governments” for “tightening the screws” on U.S. tech firms and warned that overregulation could stifle a transformative industry.

U.S. lawmakers—including House Judiciary Chair Jim Jordan (R-OH)—have echoed these remarks, arguing that EU digital rules such as the EU Digital Services Act (DSA) and Digital Markets Act (DMA) disproportionately impact U.S. companies and act “as a European tax”. House Energy and Commerce Chair Brett Guthrie (R-KY)

also has warned that the U.S. should not “regulate like Europe,” citing frameworks allegedly designed to disadvantage American firms, particularly in competition with China.

EU officials have rejected these claims. Commissioner Virkkunen called the idea that EU laws target U.S. firms “very misleading,” and Executive Vice President Ribera has emphasized that enforcement is consistent and not politically motivated.

- 3. Speech and Content Governance:** Tensions have also emerged around content moderation under the DSA, especially where AI is used to generate or manage user-facing content. U.S. officials, including FCC Commissioner Brendan Carr and Rep. Jim Jordan (R-OH), have warned that DSA enforcement may infringe on Americans’ speech rights, citing concerns about extraterritorial overreach. Jordan has sought records of the Commission’s platform interactions, suggesting an effort to influence American content standards.

EU officials strongly defend the DSA as aligned with democratic values. Commissioner Virkkunen has affirmed that it supports free expression. And European lawmakers such as Pedro Sánchez and Axel Voss have emphasized the need for AI-driven content safeguards to prevent electoral interference and disinformation.

- 4. General-Purpose AI: The Draft Code of Practice:** A flashpoint of transatlantic disagreement has emerged around the EU’s latest draft Code of Practice for GPAI systems. U.S. officials have reportedly urged revisions or withdrawal, arguing that obligations such as third-party audits and data transparency go beyond the AI Act’s scope and could chill innovation. These concerns have been raised through formal diplomatic channels, including by the U.S. Mission to the EU.

EU regulators maintain the Code of Practice is essential to operationalize GPAI requirements, ensure accountability, and uphold transparency and IP standards. It was recently announced that the final version of the Code of Practice has been delayed to August 2025 to enable the EU AI Office to take on board various stakeholders’ feedback.

The U.S. administration is likely one of them, even if the EU will not admit publicly. Though voluntary on paper, the Code of Practice is expected to influence enforcement and serve as a compliance benchmark.

PART III: LEGAL IMPLICATIONS AND COMPLIANCE STRATEGY

Overall, the legal frameworks discussed in Part I and the geopolitical dynamics explored in Part II highlight the increasing complexity of transatlantic AI governance—and the corresponding need for companies to navigate overlapping and sometimes conflicting regulatory demands. The following recommendations outline strategic considerations for managing this evolving landscape.

- **Prioritize High-Risk Use Cases:** Effective compliance begins with establishing a baseline AI governance and risk management framework. Once foundational processes are in place, companies should prioritize AI systems most likely to trigger heightened regulatory obligations. Companies should focus on use cases in sectors such as human resources, financial services, healthcare, public safety, and critical infrastructure—areas frequently designated as high-risk under the EU AI Act and subject to increased scrutiny by U.S. regulators. Developers should conduct structured risk assessments early in the development cycle and ensure that these systems incorporate appropriate safeguards, including accuracy thresholds, impact assessments, and fallback or human-in-the-loop procedures.
- **Build Cross-Functional Compliance:** Create multidisciplinary AI governance teams that include legal, policy, compliance, engineering, privacy, and operations personnel. This collaboration is essential for mapping AI system lifecycles, identifying applicable obligations, monitoring outputs, and implementing safeguards such as

human-in-the-loop oversight, documentation protocols, security measures and explainability measures. Internal alignment ensures consistent application of standards and facilitates smoother regulatory engagement.

- **Understand EU Requalification Triggers:** Entities that significantly modify, deploy, or distribute AI systems within the EU must carefully assess whether their activities could reclassify them as a “provider” under the EU AI Act. Requalification triggers—such as functional changes, repurposing for high-risk uses, or integration into broader systems—can shift the full burden of compliance. Companies should establish internal review procedures to flag changes that may implicate this reclassification risk.
- **Prepare for GPAI Obligations:** Developers and deployers of large-scale, GPAI models should proactively align with the relevant EU AI Act’s requirements in accordance with the legal implementation timeline (from August 2025) and ahead of formal enforcement (early August 2026). This includes preparing detailed technical documentation, tracking data provenance, establishing risk and performance monitoring protocols, and ensuring compliance with intellectual property, data protection and transparency obligations. Given the likely influence of the draft GPAI Code of Practice, voluntary adherence may offer both compliance and reputational benefits.
- **Engage Early with Sandboxes and National Authorities:** In the EU, regulatory sandboxes offer a controlled environment to test innovative AI systems, explore flexible compliance options, and receive feedback from national authorities. Early engagement can clarify risk classification, inform system design, and demonstrate a proactive compliance posture—potentially facilitating smoother market entry and reduced liability exposure.
- **Adapt to U.S. State Law Variability:** With no overarching federal AI law, U.S. companies must closely monitor and adapt to emerging state-level legislation. Key areas of divergence include definitions of automated decision-making, disclosure requirements, data governance rules, and enforcement mechanisms. Establishing state-by-state compliance playbooks and engaging with state regulators can help preempt enforcement risks and build trust with consumers and policymakers.
- **Embed Risk Management Frameworks:** Regardless of jurisdiction, companies should institutionalize AI-specific risk management programs aligned with global best practices. These include privacy impact assessments, red teaming for adversarial testing, bias audits, incident response protocols, and continuous monitoring. Embedding these mechanisms early in system development can mitigate harm, facilitate regulatory reporting, and strengthen internal accountability.
- **Ensure Accuracy and Avoid AI-Washing:** Overstating the capabilities or autonomy of AI systems—whether in investor materials, marketing, or public disclosures—can create reputational, legal, and enforcement risks. Ensure that claims about system functionality, safety, and independence are accurate, evidence-based, and aligned with actual performance metrics. Consider establishing internal review processes for all public-facing statements on AI.
- **Tailor for Government Contracts:** Companies contracting with U.S. federal agencies or AI procurement in the EU must navigate evolving acquisition requirements, including those outlined in [OMB Memorandum M-25-21](#) and the EU’s [Model Contractual Clauses for AI Procurement \(MCC-AI\)](#). These efforts aim to standardize expectations around responsible AI procurement and reflect a growing federal emphasis on lifecycle risk management, transparency, and vendor accountability. Key obligations include demonstrating risk mitigation strategies for high-impact AI systems, defining data rights and intellectual property protections, and addressing concerns around vendor lock-in and system interoperability. Tailoring compliance documentation and contractual terms to agency-specific implementations of these frameworks can improve competitiveness and reduce the risk of procurement delays or disqualification.

By building compliance strategies tailored to risk, geography, and system function—and treating governance as core legal infrastructure—companies can better navigate the fragmented global AI regulatory landscape while staying responsive to evolving political and legal dynamics.

CONCLUSION

The accelerating divergence between EU and U.S. AI governance—and the political tensions it has sparked—will continue to shape global compliance expectations. But while fragmentation poses challenges, it also offers opportunities for companies that approach compliance not as a constraint, but as a tool for strategic positioning.

By embedding risk management into AI development, aligning early with supervisory expectations, and tailoring governance structures to jurisdiction-specific obligations, companies can build legal resilience while maintaining operational agility. More importantly, doing so positions them to influence and adapt to emerging standards as AI oversight continues to evolve—both within and across borders.

King & Spalding's experienced cross-border regulatory team is uniquely positioned to help companies navigate this shifting terrain. With deep experience in AI, data governance, international compliance, and government engagement, we provide strategic counsel that integrates legal risk management with operational execution—enabling clients to move confidently across the transatlantic divide.

As governments race to define the future of AI, organizations that treat governance as core infrastructure—not just regulatory overhead—will be best placed to lead.

ABOUT KING & SPALDING

Celebrating more than 140 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,300 lawyers in 24 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."

View our [Privacy Notice](#).

Special Matters & Government Investigations Partners

Gary Adamson
New York
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
New York
+1 212 556 2376
abaker@kslaw.com

J.C. Boggs
Washington, DC
+1 202 626 2383
jboggs@kslaw.com

Christopher C. Burris
Atlanta
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
New York
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
Northern Virginia
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
Washington, DC
+1 202 661 7828
mciatti@kslaw.com

Daniel R. Coats
Washington, DC
+1 202 626 2642
dcoats@kslaw.com

Patrick M. Collins
Chicago
+1 312 764 6901
pcollins@kslaw.com

Ander M. Crenshaw
Washington, DC
+1 202 626 8996
acrenshaw@kslaw.com

Sumon Dantiki
Washington, DC
+1 202 626 5591
sdantiki@kslaw.com

Dan Donovan
Washington, DC
+1 202 626 7815
ddonovan@kslaw.com

Robert L. Ehrlich, Jr.
Washington, DC
+1 202 626 9710
rehrllich@kslaw.com

David Farber
Washington, DC
+1 202 626 2941
dfarber@kslaw.com

Zachary Fardon
Chicago
+1 312 764 6960
zfardon@kslaw.com

Lucas Fields
Washington, DC
+1 202 626 2399
lfields@kslaw.com

Emily Gordy
Washington, DC
+1 202 626 8974
egordy@kslaw.com

Leah B. Grossi
Washington, DC
+1 202 626 5511
lgrossi@kslaw.com

Ehren Halse
San Francisco
+1 415 318 1216
ehalse@kslaw.com

Max Hill, K.C.
London
+44 20 7551 2130
mhill@kslaw.com

Amy Schuller Hitchcock
Sacramento/San Francisco
+1 916 321 4819
ahitchcock@kslaw.com

John A. Horn
Atlanta
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
New York
+1 212 556 2278
ahruska@kslaw.com

Rob Hur
Washington, DC
+1 202 383 8969
rhur@kslaw.com

Mark A. Jensen
Washington, DC
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
Washington, DC
+1 202 626 8984
djohnson@kslaw.com

William Johnson
New York
+1 212 556 2125
wjohnson@kslaw.com

Barry Kamar
Miami
+1 305 462 6044
bkamar@kslaw.com

Allison F. Kassir
Washington, DC
+1 202 626 5600
akassir@kslaw.com

M. Alexander (Alec) Koch
Washington, DC
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
New York
+1 212 556 2207
ykotlarsky@kslaw.com

Steve Kupka
Washington, DC
+1 202 626 5518
skupka@kslaw.com

Jade R. Lambert
Chicago
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
Los Angeles
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
Washington, DC
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
New York
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
Houston
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
Atlanta
+1 404 572 2447
alipson@kslaw.com

Daniel E. Lungren
Washington, DC
+1 202 626 9120
dlungren@kslaw.com

William S. McClintock
Washington, DC
+1 202 626 2922
wmcclintock@kslaw.com

Amelia Medina
Atlanta
+1 404 572 2747
amedina@kslaw.com

Kendrick B. Meek
Washington, DC
+212 626 5613
kmeek@kslaw.com

Andrew Michaelson
New York
+212 790 5358
amichaelson@kslaw.com

Nema Milaninia
Washington, DC
+202 626 9273
nmilaninia@kslaw.com

Jim C. Miller III
Washington, DC
+1 202 626 5580
jmiller@kslaw.com

Patrick Montgomery
Washington, DC
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
Atlanta/Washington, DC
+1 404 572 4730
pbmurphy@kslaw.com

Patrick J. Murphy
Washington, DC
+1 202 626 9248
pmurphy@kslaw.com

Grant W. Nichols
Austin/Washington, DC
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
Washington, DC
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
Chicago
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
Washington, DC
+1 202 626 3732
mpauze@kslaw.com

Michael A. Plotnick
Washington, DC
+1 202 626 3736
mplotnick@kslaw.com

Olivia Radin
New York
+1 212 556 2138
oradin@kslaw.com

John C. Richter
Washington, DC
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
Washington, DC
+1 202 626 9220
rrosenstein@kslaw.com

Daniel C. Sale
Washington, DC
+1 202 626 2900
dsale@kslaw.com

Heather Saul
Atlanta
+1 404 572 2704
hsaul@kslaw.com

Greg Scott
Sacramento/San Francisco
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
Singapore
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
New York
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
San Francisco
+1 415 318 1221
mshepard@kslaw.com

Thomas Spulak
Miami
+1 305 462 6023
tspulak@kslaw.com

Aaron Stephens
London
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
Denver
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
Paris
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
Washington, DC
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
Northern Virginia
+1 703 245 1018
rvacura@kslaw.com

Anthony A. Williams
Washington, DC
+1 202 626 3730
awilliams@kslaw.com

David K. Willingham
Los Angeles
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
Washington, DC
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
Atlanta/Washington, DC
+1 404 572 2723
syates@kslaw.com

Joseph Zales
New York
+1 212 827 4087
jzales@kslaw.com