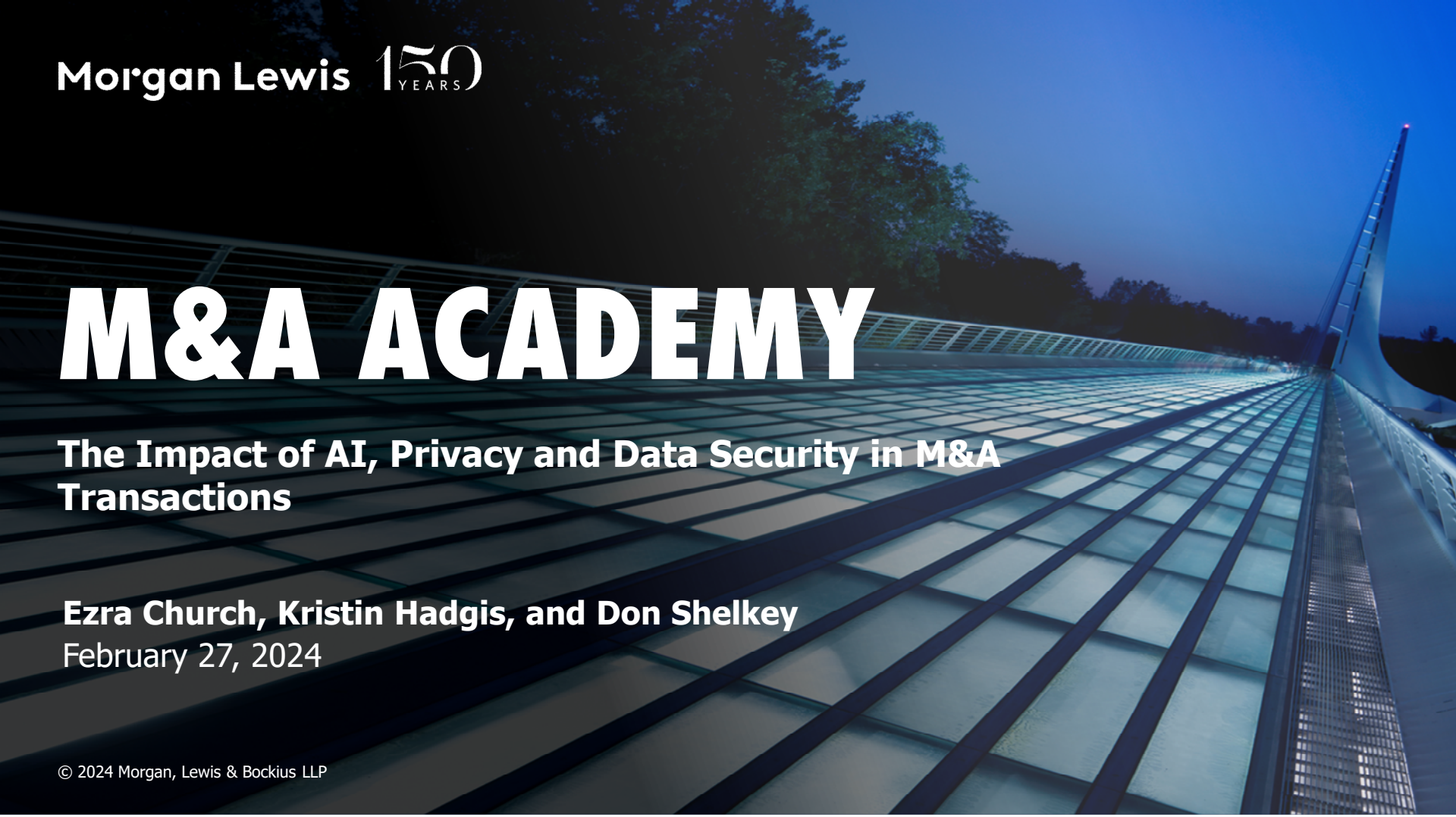

Morgan Lewis
150 YEARS
M&A ACADEMY
The Impact of AI, Privacy and Data Security in M&A Transactions
Ezra Church, Kristin Hadgis, and Don Shelkey
February 27, 2024
© 2024 Morgan, Lewis & Bockius LLP

Overview

- Introduction
- Why should I care?
- Five Key Legal Requirements
  - Sector-Specific laws
  - Privacy Policies
  - Data Security Requirements
  - Breach Notification Laws
  - International Privacy Rules / Cross-Border Restrictions
- Implementing Privacy and Security in Deals
  - Diligence
  - Reps and Warranties
  - TSAs

Why should I care?

- If a target company cannot collect and deploy data consistent with data privacy laws, there may be flaws in the premise for the deal or the business model itself
- Failure of target company to meet its data privacy and security obligations can be a major risk for acquiring company
- Transfer and sharing of data in connection with diligence and after the transaction may in itself violate data privacy laws

Good News / Bad News

- **Good News** – there is no all-encompassing data privacy or cybersecurity statute in the U.S.; the GDPR applies across Europe (with local laws)
- **Bad News** – there is no all encompassing data privacy cybersecurity statute in the U.S.; the GDPR applies across Europe:

Attorney General Enforcement
FTC Act
FCRA
CAN-SPAM
COPPA
Breach Notification Laws
Data Disposal Laws
FERPA
Gramm-Leach-Bliley
MA Data Security Regulations
Red Flags Rule
FACTA
EU “safe harbor” rules
Consumer Class Actions
PCI and DSS Credit Card Rules
Document Retention Requirements

HIPAA
CA Online Privacy Act
CA Consumer Privacy Act
Stored Communications Act / ECPA
Do Not Call Lists
Telephone Consumer Protection Act
Video Privacy Protection Act
Wire Tapping liability
Invasion of Privacy Torts
Computer Fraud and Abuse Act
Communications Decency Act
Spyware Laws
RFID Statutes
FDCPA
Driver’s Privacy Act
Social Security Number Laws
Others State Laws

1. Sector / Jurisdiction Specific US Privacy Laws

Money	Health	Kids	California (and other states)
• Gramm-Leach-Bliley Act • Fair Credit Reporting Act (FCRA) • State Laws	• Health Insurance Portability & Accountability Act (HIPAA)	• Family Educational Rights & Privacy Act (FERPA) • Children's Online Privacy Protection Act (COPPA) • State Laws	• California Consumer Privacy Act

- Consumer Marketing! Telephone Consumer Protection Act (TCPA), CAN-SPAM, and Do Not Call regulations
- Biometrics

California Consumer Privacy Act

- First law of its kind in the US; effective January 1, 2020
- Applies to a **business** which: (1) has annual gross revenues in excess of $25 million; (2) annually buys, receives, sells or shares personal information of 50,000 or more consumers, households, or devices, alone or incomgination; (3) **or** derives 50% or more of its annual revenue from selling consumers' personal information.
- Requires privacy notices be provided at the time personal information is collected
- Consumers also include employees, job applicants, contractors and business contacts
- Gives consumers rights, including:
  - Right to know specific pieces of personal information collected about the consumer in the preceding 12 months
  - Right to delete personal information
  - Right to opt out of sale of personal information
  - Right to a website privacy policy that describes how to exercise these privacy rights
- Requires certain language in contracts with "service providers"

Beyond California—More State Consumer Privacy Acts

- In addition to California, four other states have consumer privacy laws currently in effect:
  - **Virginia**
  - **Colorado**
  - **Connecticut**
  - **Utah**
- Flurry of new consumer privacy laws enacted in 2023, with the following effective dates:
  - **Oregon** – July 1, 2024
  - **Texas** – July 1, 2024
  - **Montana** – October 1, 2024
  - **Delaware** – January 1, 2025
  - **Iowa** – January 1, 2025
  - **Tennessee** – July 1, 2025
  - **Indiana** – January 1, 2026
- Unlike California, these laws do not apply to information collected from employees, job applicants, contractors and business contacts.

2. Privacy Policies—US

- FTC and State Laws (e.g., CA, NV & DE)
- Self-imposed regulation
- Basic principles
  - Notice
  - Access and Control
- Must notify regarding material, retroactive changes
- Language to look for:
  - "Transfer of assets" language
  - Restrictions on sharing/sale of personal information
  - Promises about security
- Look at the language for all entities involved over time; website and mobile
- Other public statements about privacy and security?

> Unfair and deceptive acts or practices in or affecting commerce . . .
> Are declared unlawful.
>
> — SEC. 5, FEDERAL TRADE COMMISSION ACT

3. Data Security Requirements

- US Sector-specific laws may apply
- GDPR requirement for technical and organizational measures to protect personal data
- Contracts may require certain security standards – NB EU/UK data processing agreements must include security obligations

- MA Security Regulations
  - Have a written information security plan
  - Additional administrative discipline
  - Social security numbers
  - Encryption
  - Training

4. Breach Notification—US

- 50 States and D.C.
- Based on the individual's residence
- Triggering elements vary
- Encryption / lack of use exception – sometimes
- Timing of notice– "as soon as practicable," but
  need information to notify
- Vendor management

5. International Privacy Rules / Cross Border Data Transfers

- **EU/UK GDPR**
- The GDPR applies to processors and controllers having an EU/UK-based establishment
- The GDPR also applies to controllers and processors based outside the EU/UK territory where the processing of personal data regarding EU/UK data subjects
- Fines are significant: the higher of 4% of global revenue or €20 million/£17.5 million for breaches (likely to be long-standing and significant breaches at the maximum end of potential penalties).
- **Transfers out of EU/UK**
  - Transfers of EU/UK personal information out of those jurisdictions is PROHIBITED unless special protections or exceptions are in place.
  - Standard contractual clause agreements: good, but need risk assessments and consider additional safeguards and suspension of data flow rights if risks are too high.
  - EU/US Data Privacy Framework: Companies can certify compliance with basic EU data protection principles with the U.S. Department of Commerce
  - Consent of Data Subjects: really only works at an individual level; consent must be freely given/fully informed and can be revoked at will
  - Necessary for Contract Performance or litigation purposes: limited to "necessary" transfers e.g. address for shipping or a legal dispute (may need to review data before transfer so only necessary data is transferred).
- **APEC Countries**
  - Chinese Personal Information Protection Law (PIPL) prohibits transfer out of China in some cases
  - Data processing and sharing restrictions in many countries e.g. Australia, India, Singapore, Dubai, Bahrain, Japan, Brazil

M&A - Reps and Warranties

- Privacy and Security related reps and warranties are most often included in the "Intellectual Property" section.
- Common Privacy related reps:
  - Compliance. Seller is in material compliance with all applicable Laws, as well as its own rules, policies and procedures, relating to privacy, data protection, and the collection, use, storage and disposal of personal information collected, used, or held for use by Sellers in the conduct of the Business.
  - No breaches. There has been no unauthorized access to or acquisition of personal information processed by the Seller or on Seller's behalf.
  - Claims. No claim, action or proceeding has been asserted in writing or, to the Knowledge of Seller, threatened in connection with the operation of the Business alleging a violation of any Person's rights of publicity or privacy or personal information or data rights.
  - Security. Seller has taken reasonable measures, including, any measures required by any applicable Laws, to ensure that personal information used in the conduct of the Business is protected against unauthorized access, use, modification, or other misuse.
  - Transaction compliance. The transaction itself, including execution of the related documents will not violate privacy laws or any contract or other commitment of Seller.
  - Known vulnerabilities. For technology / software heavy deals, there are no vulnerabilities in the NIST NVD.

M&A - Privacy related Diligence (Buy Side)

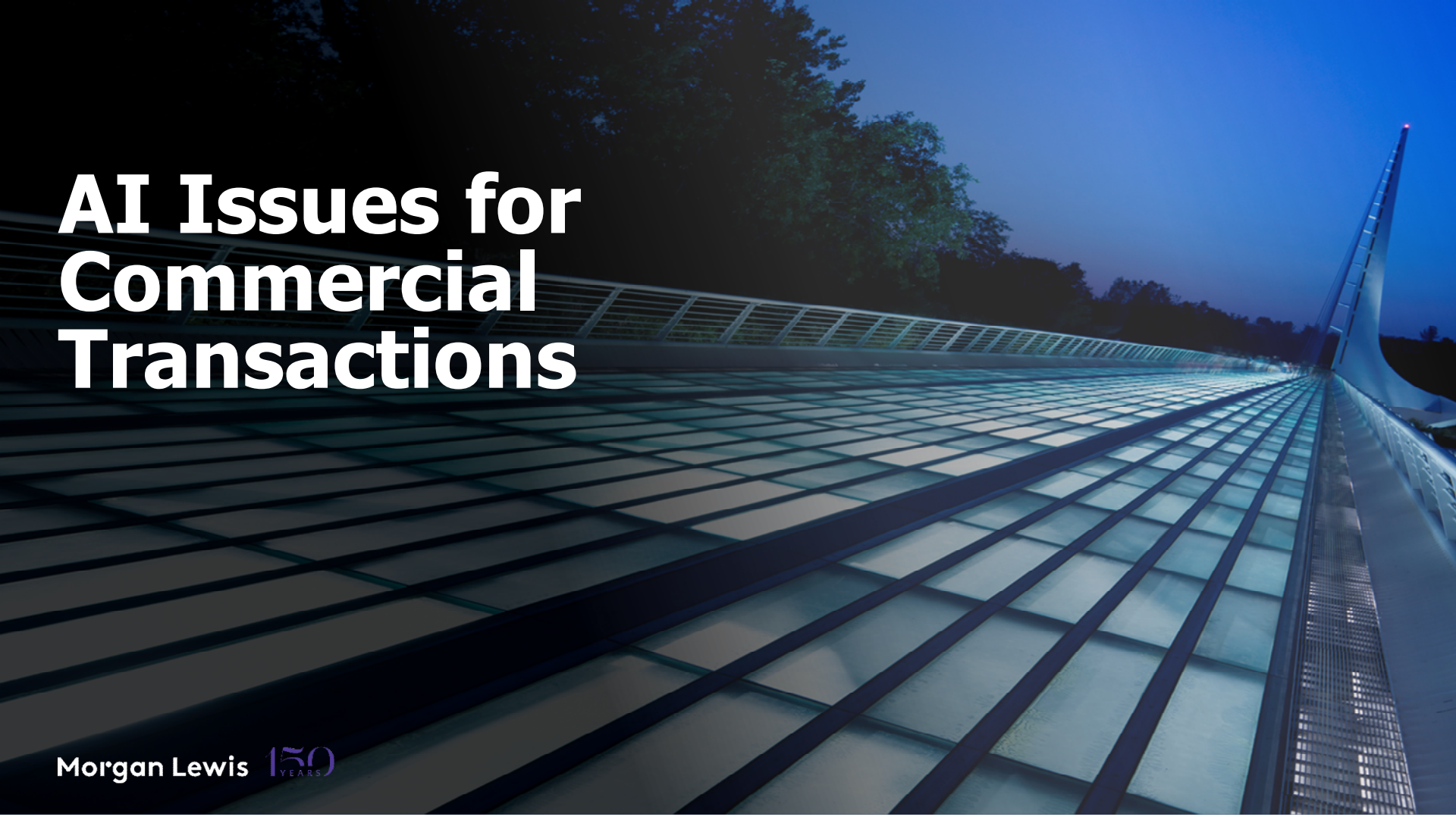
- Scope and effort driven by risk profile.
- Review privacy policies and contracts.
- Review compliance with industry, data, and jurisdiction-specific rules (Money, Health, Kids, Consumer Marketing, EU/UK data).
  - Consider discussion with privacy officer / privacy counsel.
- Review security-related documents for red flags.
- Review any data braches carefully, incl. response planning and team, vulnerability scans, audits; ask hard questions.
- Rep and warranty insurers will focus on privacy and security , particularly EU and credit card data.

M&A - Privacy related Diligence (Sell Side)

- Address it head on and project confidence, particularly in regulated industries or retail, uploading privacy policies to the data room and describing data collection and transfer issues.
- Identify potential problem areas and develop a strategy, particularly on breaches, class actions, and government investigations.
  - Keep / develop logs of any data security breaches, remediation efforts, and steps to prevent in the future.

M&A - TSAs

- Transition Services Agreements; common in M&A transactions.
  - Not done with privacy just because a deal is signed / closed.
  - Often involve some of the most sensitive data that the company (employee data, customer data).
  - Involve a member of the privacy team early when discussing the TSA.
  - Could require an information security audit from Buyer (which is somewhat counter intuitive)
  - The Seller is likely to be a processor so an EU/UK data processing agreement may be needed (can be included in the TSA)
  - Think of them as an outsourcing or hosting deal…the issues are the same!


AI Issues for Commercial Transactions
Morgan Lewis
150 YEARS

Topics

- Guiding Principals
- Non-AI Deals - Outgoing Data
- Non-AI Deals - Work Product Generation
- AI Deals

Honorable Mention: AI Usage Policies

Guiding Principles

- Disclosure of Use
  - Allows your organization to adapt to the changing regulatory landscape
  - Corporate activity
  - Relationship Issues
  - Allows appropriate approval and escalation

- Independent Human Verification
  - AI is a tool, not a substitute for professional judgment
  - Not always possible or appropriate. Consider use case.

Protecting your Outgoing Data

- Why do we care?

- Beware of permitting use of your data generally to "improve the services."
- Prohibit data from being used to seed, train or improve AI (even if anonymous).

- "*In no event will Supplier use any Client Data, or derivatives thereof (whether or not such Client Data has been anonymized or deidentified), to train or improve any algorithm or model used in any artificial intelligence product or services without Client's prior written consent.*"

Vendor Work Product

- Why do we care?

- Beware of the IP (copyright infringement) and OS (viral) risks.
- Require consent if AI is used to create work product.

- "*In no event will Supplier use any artificial intelligence, including generative artificial intelligence, products or services to perform the Services or generate or produce any Deliverables (or any components thereof) without the express prior written consent of Client.*"

What about AI Deals?

- “As a condition to use by Supplier of any artificial intelligence products or services, Supplier must ensure that (i) Supplier has full rights and licenses to such products and services, (ii) Supplier obtains all Intellectual Property rights and all rights and title to the output of or from such products and services, and that it may transfer such ownership of such output to Client if included in any Deliverable, and (iii) Supplier is solely responsible for verifying and ensuring the quality and accuracy of any the output of from such products and services.”

- Don’t forget compliance with laws. They are changing!

Some Notes on AI Policies

- Private systems vs Public systems.
- Disclosure of use is a powerful tool.
- Independent Human Verification. Think Google or Bing with two caveats:
  - A reader can tell if you used AI
  - Careful of uploading personal information or client information
- Level of approvals for various tools. (Include GC)
- All work product (especially legal) must be independently reviewed.
- Legal team is not exempt from this.

QUESTIONS?

Biography

Ezra D. Church
Philadelphia, PA
T +1.215.963.5710
F +1.215.963.5001

Ezra D. Church counsels and defends companies in privacy, cybersecurity, and other consumer protection matters. He helps clients manage data security and other crisis incidents and represents them in high-profile privacy and other class actions. Focused particularly on retail, ecommerce, and other consumer-facing firms, his practice is at the forefront of issues such as biometrics, artificial intelligence, location tracking, ad tech, and blockchain. Ezra is leader of the firm's privacy and cybersecurity litigation practice and co-chair of the firm's Class Action Working Group.

Biography

Kristin M. Hadgis
Philadelphia, PA
T +1.215.963.5563
F +1.215.963.5001

Kristin M. Hadgis counsels and defends retail and other consumer-facing companies in matters relating to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, retail operations, loyalty and gift card programs, and commercial disputes. Kristin also handles data security incident response crisis management, including any resulting litigation or government investigations.

Biography

Doneld G. Shelkey
Pittsburgh, PA
T +1.617.341.7599
F +1.617.341.7701

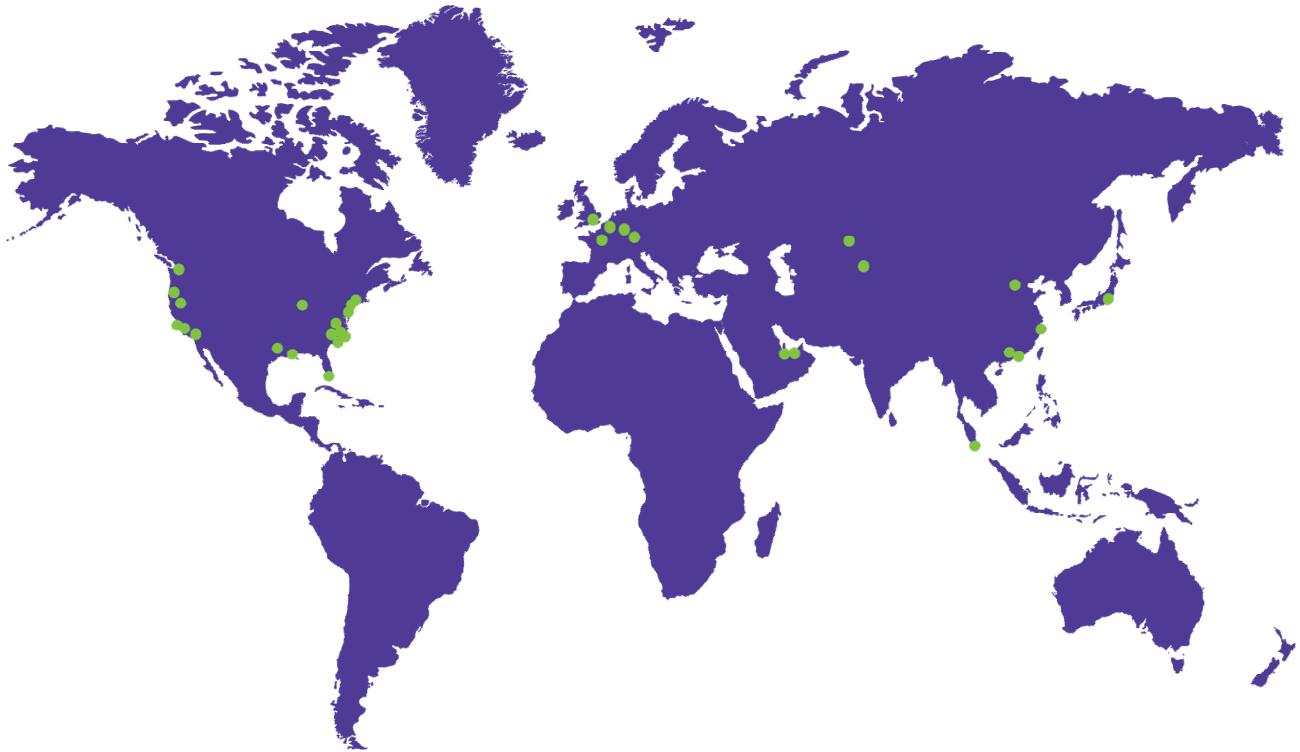
Don Shelkey is the global leader of the firm's technology transactions, outsourcing, and commercial contracts (TOC) practice. Don represents clients across a wide array of complex and strategic transactions involving intellectual property, technology, and other commercial matters. Don regularly negotiates deals that focus on artificial intelligence (AI), data rights, assets, software as a service (SaaS), cloud computing, data acquisition and services, enterprise resource planning (ERP), blockchain, software licensing and development, social media, sponsorships, and strategic joint ventures and business collaborations. He advises on AI-related issues, including AI policy creation, contract negotiation, issue spotting, representations and warranties–related issues, and AI-related diligence support.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Astana
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong
Houston
London
Los Angeles
Miami
Munich
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai
Shenzhen
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis 150 YEARS

THANK YOU