NOVEMBER 12, 2025

CLE CONTINUING LEGAL EDUCATION

Optimizing AI Investments

Protecting Value and Managing Risk Through Diligence

Presentation for *Privacy+Security Forum Fall 2025*

WILLKIE

Investing in AI Companies

Benefits and Risks

- AI is now a strategic business imperative given its wide range of use cases
  - These use cases include risk management, customer relationship development, coding/engineering/product development, cybersecurity, and many more
- Investments in AI companies have increased since the popularization of generative AI
  - In 2024, one out of every three venture capital dollars invested globally went to an AI startups
  - In North America, AI companies grabbed nearly half of all VC dollars.
- AI assets can be a huge source of value and also unique risk
  - Regulatory risk, technical understanding of the models, IP ownership of data and models, data quality and use, etc.

Due diligence of AI assets is key to ensure that investors are buying value, not volatility.

Benefits of Proper Due Diligence

- ✓ Risk Mitigation
- ✓ Valuation Accuracy
- ✓ Integration Planning
- ✓ Regulatory Compliance
- ✓ Clear Understanding of Existing and Potential Future Use Cases
- ✓ Ensuring AI Capabilities Match the Company's Claims about its AI Use
- ✓ Validates IP Ownership and Licensing
- ✓ Protecting the Investment Value

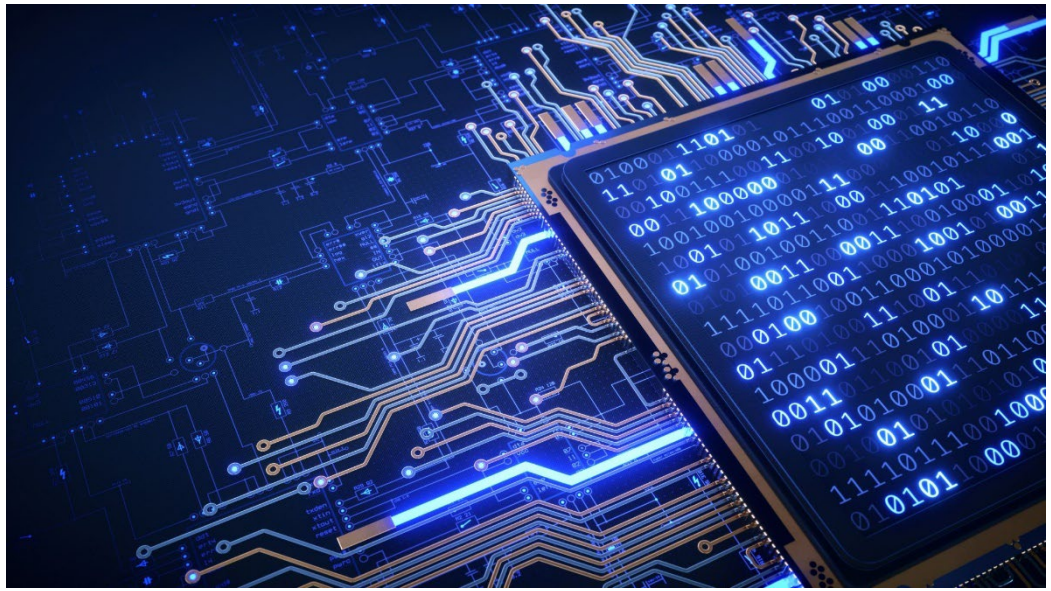
Key Issues in Diligence

WILLKIE

Key Diligence Questions

These are key issues that should be reviewed in diligence

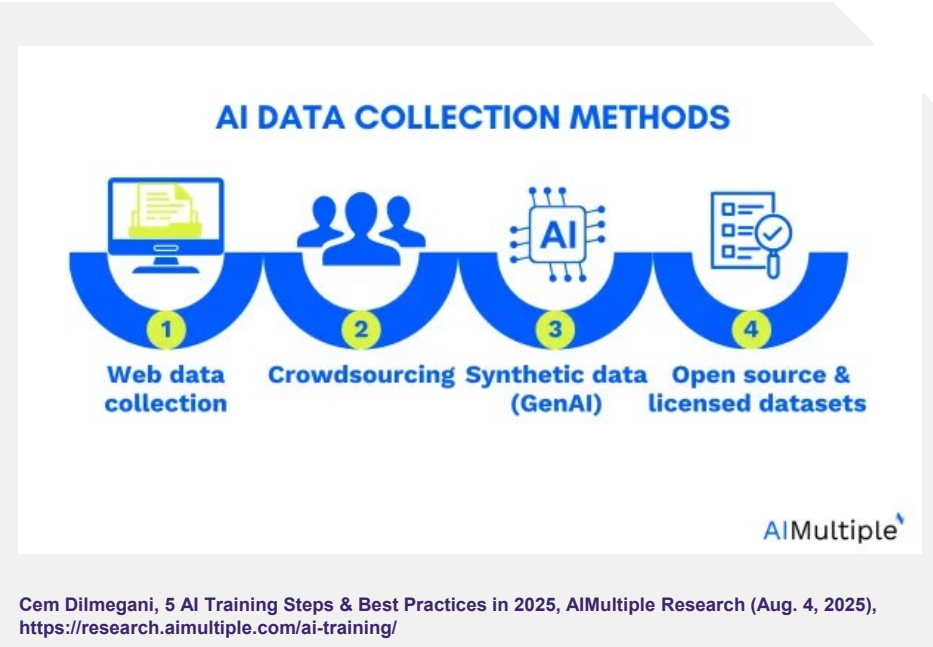
- Are the models licensed or proprietary?
- What restrictions are imposed on the use of AI inputs and outputs?
- How and from where does the company obtain training data?
- Are the AI systems explainable and auditable?
- What policies and procedures does the company have in place to manage compliance with developing AI laws?
- Does the company's AI model actually do what is advertised?



Data Sources and Uses

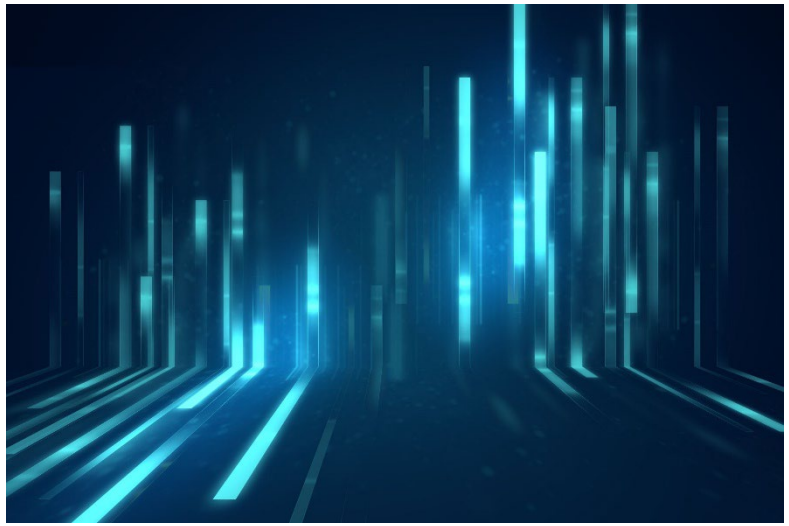
AI is driven by data

- Data comes from many sources, and the use/ownership of that data must be clear
- If company is subcontracting the operation of AI tools, then reviewing rights, limitations, and obligations of relevant contracts is necessary
- Companies could be in breach of those contracts concerning use/ownership of data



Cem Dilmegani, 5 AI Training Steps & Best Practices in 2025, AIMultiple Research (Aug. 4, 2025), https://research.aimultiple.com/ai-training/

Use and Ownership of Inputs and Outputs



- Contracts or licenses may prohibit data disclosure or certain uses, including using data for AI training
- Outputs should be validated, logged, monitored and audited
- Are the AI outputs proprietary?
- Are there limitations on the use of AI outputs by third parties/customers?

Ownership of the AI Model/Product

Patentability, Copyright, and Trade Secret Protections are still developing in this area

- Ownership of models and product—does the company properly own all aspects?
- Use of open source or pretrained models—are licenses compatible with commercial use?
- AI code written by contractors or third parties and assignment issues
- Patentability, copyright, or trade secret protections of AI tools

AI-Related Patent Applications are up 33% since 2018

US Copyright Lawsuits Against AI Companies

Key Lawsuits

Authors Guild v. Open AI (Sept. 19, 2023-SDNY)

The Authors Guild, along with many prominent authors, alleges that OpenAI infringed upon their copyrights by using their literary works without permission to train its AI models

December 4, 2023 - Authors Guild filed an amended complaint adding Microsoft as a defendant, alleging its involvement in the development and deployment of OpenAI's models

Issues: whether (i) OpenAI's use of copyrighted books constitutes infringement, (ii) AI outputs qualify as unauthorized derivative works, and (iii) the fair use defense is applicable

Getty Images v. Stability AI (Feb. 2, 2023-D.Del.)

Getty Images accuses Stability AI of infringing its copyrights by using over 12 million of its photographs, along with associated captions and metadata, to train and develop the Stable Diffusion model

July 8, 2024 - Getty Images filed a second amended complaint adding Stability AI US Services Corp. as a defendant, dropping one DMCA claim but maintaining copyright, trademark, and unfair competition claims

Issue: whether Stability AI's use of Getty's images to train its models constitutes copyright or trademark infringement

Sarah Andersen v. Stability AI (Jan. 13, 2023-N.D.Cal.)

Artists Sarah Andersen, Kelly McKernan, and Karla Ortiz filed a class-action lawsuit alleging that Stability AI, Midjourney, and DeviantArt infringed their copyright by using their artwork without consent to train AI image-generating platforms like Stable Diffusion

October 31, 2024 - the plaintiffs filed a second amended complaint expanding claims against Stability AI, Midjourney, Runway AI, and DeviantArt for copyright and DMCA violations across model training and output, while removing unjust enrichment and breach of contract claims from the previous complaint

Issue: whether use of the artwork by the defendants constitutes copyright infringement

Example of Data Use Issues in Corporate Deal

Diligence about a company's use of customer data to train AI model was key

- Client was investing in a cyber resilience platform that relies on a proprietary AI model as a key component of its services.
- Issue? Diligence uncovered that the Company had significant limitations in customer contracts regarding use of customer data to train AI systems.
  - BUT…customer data was critical in the development of the Company's AI tools and features
- Solution? Specific representations about the use of data, as well as indemnities covering any claims related to or arising from the Company's use of data, for the purposes of training, developing, and/or using AI Technologies, including any future training, developing, or use of AI Technologies by the Company.
  - Allowed the investment to move forward, with robust risk protection for investors.

Infrastructure

AI can require a lot of computing power, IT investment, and other infrastructure

- Assessing compute infrastructure is important to verify that the company can support scaling AI use/development
- Inadequate AI development practices
  - The absence of explainability measures and risk mitigation approaches could be red flags
  - Remediation may require development of IT policies and procedures
- Identifying key personnel is critical for transition

Risks Under Existing Laws

There are a number of existing laws that may impact the use, development, and training of AI

- In the US, the FTC, SEC, and other regulators have used existing authorities in the AI context.
  - SEC, FTC had prioritized enforcement against “AI washing”, i.e., unfair or deceptive uses or claims regarding AI.
  - FTC has said that use of AI should be:
    - ✓Transparent
    - ✓Explainable
    - ✓Fair
    - ✓Empirically Sound
    - ✓Non-discriminatory
    - ✓Accountable
- Privacy laws, discrimination laws, trademark/copyright/patent laws, and other laws in the US and globally may impact the use of personal data or other confidential data in AI models

A Closer Look at Regulating AI via Privacy Law

Privacy laws in Europe, the UK, and several US states indirectly regulate AI by regulating the personal data used in AI systems

Consumers' rights over personal data or personal information apply to that data used in AI products

- Rights to deletion, access, correction
- May also be required to provide users the opportunity to restrict processing of certain types of data or otherwise limit certain uses of data
- Must disclose the types of data an AI product uses, and the reasons why

Under GDPR (in the EU and UK), lawful basis required for processing personal data

GDPR also includes requirements specific to "automated decisions" – data subjects must be able to opt-out of decisions "based solely on automated processing, including profiling, which produces legal effects concerning" the data subject.

"Sensitive" Data

Processing certain types of "sensitive" personal information (e.g. biometric information, racial or ethnic information, sexual orientation) may require additional protections or is subject to additional limitations.

Understanding the scope of the company's personal data collection and processing are critical to scoping the risk and potential liabilities presented by a particular company's practices.

Evolving Regulatory Landscape

The US and other countries are proposing and enacting AI-specific laws

- Developing laws and regulations globally that are aimed at curbing potential abuse and misuse of AI tools
- Many focused on "high-risk" uses.
  - E.g., offering a job or promotion, determining whether an individual is eligible for a financial product, healthcare, critical infrastructure, or education
- Diligence can help investors understand the extent to which regulation may present challenges for a company's growth.

Colorado AI Law
US

EU AI Act
EU

Interim Measures for the Management of Generative Artificial Intelligence Services
China

Act on Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies
Japan

And more on the horizon…

Governance and Risk Management

- Every company should have a governance framework in place to help manage AI-risk
- Even if company is not AI-centric, an AI-specific use policy helps manage employees' use of AI for business purposes
- Companies with AI-specific policies are better positioned to successfully manage both the risks we know about, and the risks waiting over the horizon
- NIST AI Risk Management Framework can be a helpful foundation to assess and manage AI risks

Potential Impacts of Diligence

WILLKIE

Poor AI Diligence

What could go wrong?

- Increased litigation risk
- Increased enforcement risk
  - The FTC and other US state and federal regulators have secured data disgorgement in consent decrees, large fines, and other key enforcement actions.
  - Global enforcement risk – regulators around the world imposing both monetary and equitable remedies, including banning products that do not comply with local laws.
- AI products and services fail to meet promised potential
- Failed investments

Comprehensive AI diligence

Solve current issues and prevent future issues

- Verification of promised AI product/service potential
- Identification and remediation of key issues
  - Lack of IT structure, policies, or procedures → Development in pre-closing period
  - Key personnel need to be transitioned → Negotiation of such transition
  - Data Restrictions → Negotiation of purchase agreement representations and indemnification
  - Other red flags may call for renegotiation of key deal terms and/or purchase price
- Protecting the value of the company assets and business

Questions?

WILLKIE

Your Presenters

Daniel Alvarez

dalvarez@willkie.com
202 303 1125

Daniel is Co-Chair of Willkie's Privacy, Cybersecurity & Data Strategy Practice Group.

His practice focuses on advising and representing companies on matters related to innovative data uses, privacy, data protection, and cybersecurity—including developing policies and procedures related to the collection, use, and security of data, developing and negotiating vendor and customer contracts involving data transfers, and conducting risk assessments related to automated decision-making, artificial intelligence, and other, similar activities. Drawing on a broad range of experience from different positions in government, Daniel helps clients navigate the legal, policy, and regulatory issues raised by different potential data collection and processing activities.

Genevieve Dorment

gdorment@willkie.com
212 728 3865

Genevieve is a partner in Willkie's Intellectual Property Department. She has extensive experience advising companies, private equity firms and exempt organizations in all intellectual property and technology aspects of corporate transactions, including mergers and acquisitions, capital markets and financing transactions, licensing, strategic agreements and U.S. trademark prosecution enforcement.

Genevieve has given lectures for the New York City Bar Association, and the American Law Institute, and has served as a group leader in Leading Women in Technology's WILpower leadership program.

Spencer Simon

ssimon@willkie.com
212 728 8525

Spencer is a partner in Willkie's Intellectual Property Department.

Spencer's practice focuses primarily on the representation of technology-intensive companies in all aspects of intellectual property, corporate and other commercial transactions, and data protection and cybersecurity matters. His practice covers a broad spectrum of technologies, including software, fintech, pharmaceutical, biotechnology, medical devices, semiconductor and telecommunications.