Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

10 Best Practices For Due Diligence In AI Transactions

By **Lee Tiedrich and Daniel Gurman**
(September 21, 2018, 11:39 AM EDT)

Lee Tiedrich

Daniel Gurman

Artificial intelligence is projected to contribute over $15 trillion to the global economy by 2030,[1] which in turn suggests that the number of AI-focused mergers and acquisitions, investments and other types of transactions will continue to grow. Here are 10 best practices for approaching AI-focused transactions, taking into consideration the nature of the technology today, the anticipated technological developments and the evolving legal landscape pertaining to AI.[2]

1. Understanding the Transaction

As in any transaction, it is important to identify and understand at the outset of an AI transaction the core assets that support the valuation of the target's business. For example, at its core, there are three central components to AI — the hardware, the software and the data (including training data and AI outputs). Knowing upfront which of these components is material to the target's business will help tailor the buyer's diligence, and it may influence the terms of the purchase agreement and inform the buyer of actions it may want to undertake post-closing. The following best practices provide guidance on how to tailor the due diligence to focus on the core AI assets and can inform the buyer of steps it may want to take during the negotiations or before or after the closing.

2. Intellectual Property Due Diligence

Once the core assets have been identified pursuant to best practice no. 1, the buyer should tailor its intellectual property due diligence to ascertain information about the target's rights to the material intellectual property. The following provides examples of how to tailor the IP diligence to focus on the assets that are material to the transaction.

Algorithms and Software

When substantial value is placed on the algorithms (and the software that implements the algorithms), the buyer should undertake due diligence to understand whether and to what extent the software is derived from open-source software or third-party software. Open-source audits can be helpful in these situations. The buyer also will want to assess whether the target has undertaken reasonable measures

to maintain the secrecy of this information. This is critically important because implementing such measures is a requirement for maintaining trade secret protection under U.S. law.[3]

Training Data

When substantial value is placed on the training data, the buyer should start the diligence by asking: (1) What is the core data, (2) from where is it sourced, and (3) how is it used? AI companies often obtain training data from a variety of sources, such as (1) data collected from third-party sites and services via scraping or text and data mining, (2) in-licensed data from customers or other third parties, and (3) data the company collects through its own sites and services. There has been litigation concerning web scraping practices,[4] so the buyer will want to undertake due diligence to understand the extent to which the target's practices pose a litigation risk.

For in-licensed data, it is important to assess whether the target's agreements give the target the right to use the data to train its algorithms. Because many agreements were not drafted with AI in mind, determining the target's rights to use in-licensed data as training data may require a judgment call. For the target's own data, if it is personal data, it is important to determine whether the target has obtained the appropriate consents.

AI Output

Many companies derive value from AI software output, and in these situations it is important to understand the target's rights to the output. Many companies address these issues in their customer and other commercial agreements, so review of these agreements can provide valuable information with respect to the target's rights to the AI software output.

If the agreements are not clear as to who owns the software output, there may not be a clear answer under the law. For example, software output may be copyrightable; however, who owns the copyright to software output may depend on whether the software developers or the user performed most of the work in creating and contributing to the output. Depending upon the facts and circumstances, it potentially could be difficult to identify who was responsible for most of the creativity.

3. Data Privacy Due Diligence

There are various legal frameworks that may govern the collection, use, disclosure and other processing of the data, depending upon the nature of the data (such as whether it includes personally identifiable information), the location of the data subjects, and where the data is used or otherwise processed.[5] The diligence should include an assessment of whether and to what extent the target has complied with applicable data privacy laws, particularly because failure to comply with such laws could result in, among other things, significant government fines, lawsuits and reputational harm. The diligence also should include a review of the target's privacy policies, which are relevant not only for compliance, but also may determine how the target's data can be used both before and after the closing of the transaction.[6]

4. Cybersecurity Due Diligence

A buyer should also undertake due diligence with respect to cybersecurity. As evidenced by several recent high-profile data security breaches,[7] there can be substantial adverse repercussions (including litigation, as discussed in section 7 below) if the target's data has been or is vulnerable to a data security

breach. The diligence can include an assessment of the extent to which the target's networks and systems are secure to avoid tampering or manipulation of the algorithm, training data or outputs. Typically, the cybersecurity diligence is undertaken by technical experts working closely with legal counsel to assess the legal implications of the technical expert's findings. It is also common to request results of technical third-party audits of cybersecurity practices. The diligence should include a review of the target's relevant agreements to understand its contractual rights and obligations in the event of a data security breach, particularly since the cost of remediation and the damages can be substantial should a breach occur.

5. Insurance Due Diligence

Given the risks associated with cybersecurity breaches, the buyer may want to diligence the target's insurance coverage. Diligence is important because a given cyberinsurance policy may not fully cover every type of incident thought to be cyber-related or every cost arising out of such an incident, but other policies in the target's insurance program may help fill gaps. To highlight one example, cyberinsurance policies often include a "professional services exclusion" that may limit coverage for the disclosure of third-party confidential information in a data breach. However, a technology errors and omission policy, which is designed to protect a company from liability arising out of its normal business activities, will likely fill this gap. A cybersecurity incident often implicates a patchwork of different types of insurance policies, including cyberinsurance, general liability, technology errors and omissions, property, directors and officers, and crime policies. Diligence of these policies, including all relevant limits and deductibles, can help a buyer determine the extent to which the target is adequately insured in the event of a cybersecurity breach.

6. Governance Due Diligence

A buyer also should be asking whether the target has an internal governance program intended to provide that the AI is fair and that there are appropriate accountability checks in place. For example, depending on the nature of the target's business, the buyer may want to assess the target's transparency about the factors considered by the AI algorithm and whether the training data and AI outputs are appropriate for the task at issue. This is important not only for purposes of understanding how the target's AI products function, but also for purposes of assessing legal risks. Additionally, AI governance issues have garnered attention from industry groups and policymakers, so best practices and legal requirements may continue to evolve. The buyer consequently will want to understand the level of awareness the target has with respect to governance issues and how its practices measure up in this evolving environment.

7. Product Liability Due Diligence

The buyer also should consider undertaking AI products liability due diligence. While there is limited public information regarding AI product liability litigation, the potential for such litigation certainly exists. For example, there is a risk of AI product liability litigation relating to harm caused by the AI product itself. It also was recently reported that some plaintiffs lawyers are focusing on cybersecurity practices.[8] To assess the legal risks, a buyer should undertake due diligence to evaluate how a target monitors the operations of its AI products as well as how it responds to errors and other incidents involving such products. In addition, the buyer can review the target's contracts to determine how it manages liability and risks through disclaimers, indemnifications and other contractual terms.

8. Surveillance Due Diligence

A buyer should also conduct diligence with respect to the target's compliance with surveillance laws. This is important because companies that create and host AI solutions may receive legal demands from the U.S. and other governments under surveillance laws that allow the government to obtain digital information in connection with both criminal and national security investigations. As a legal matter, companies are obligated to respond to valid law enforcement demands. If they do not, the U.S. government may enforce such requests through contempt proceedings. At the same time, a company may face civil liability if it provides information in response to a facially invalid lawful process request. To address these concerns, diligence can be undertaken to determine if a target (1) had received lawful process requests, and (2) what processes and procedures it has in place to respond to such requests.

9. Foreign Investment/National Security Due Diligence

The Committee on Foreign Investment in the United States has been closely scrutinizing investments by foreign parties in U.S. companies that are developing or possess AI and related technology (e.g., robotic and autonomous systems, big data). In August 2018, President Donald Trump signed the Foreign Investment Risk Review Modernization Act, which reformed CFIUS and expanded the committee's jurisdiction to review foreign investments (including, in some cases, small minority investments — even below 10 percent equity) in certain U.S. businesses, including many businesses involved in AI.

To the extent that an AI transaction involves foreign parties, it is important to fully evaluate CFIUS risks related to the transaction, including whether the transaction should — or must — be notified to CFIUS. If CFIUS determines that a transaction subject to its jurisdiction presents any risk to U.S. national security, the committee has broad authority to take action to address those risks, up to and including recommending that the president prohibit a transaction or, for completed transactions, require a divestiture. There is no statute of limitations on CFIUS' authorities, and no real opportunity for judicial review. Considering the potential CFIUS implications of a transaction early in the process (before a deal has been signed) also can assist the parties in structuring the transaction in a manner that reduces U.S. national security risks associated with the transaction and help them plan for seeking any CFIUS approvals that may be needed.

10. Other Regulatory Diligence

If the target's AI products operate in a regulated industry (such as autonomous vehicles, health care or financial services), the buyer may want to undertake further regulatory diligence tailored to the specific regulated industry.

Lee J. Tiedrich is a partner at Covington & Burling LLP and co-chairwoman of the firm's global interdisciplinary Artificial Intelligence Initiative.

Daniel Gurman is an associate at the firm.

The authors thank Covington attorneys Zach Mears, Jonathan Wakely, Emily Ullman, Rebecca Jacobs, Katharine Goodloe and Ani Gevorkian for their contributions to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Sizing the Prize: What's the real value of AI for your business and how can you capitalize? PricewaterhouseCoopers (2017).

[2] These best practices focus on the issues raised by AI applications and are not intended to address general corporate and other matters that are a common focus in most transactions.

[3] Uniform Trade Secret Act, Section 1(4) and the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1839(3)(A).

[4] See, e.g., hiQ Labs Inc. v. LinkedIn Corp. (N.D. Cal. Aug. 14, 2017), Fidlar Technologies v. LPS Real Estate Data Solutions (7th Cir. 2016), Cvent Inc. v. Eventbrite Inc. (E.D.Va. 2010), and Southwest Airlines Co. v. FareChase Inc. (N.D. Tex. 2004).

[5] For example, depending on location of the data gathering and processing activities, different territorial frameworks may be more important than others (e.g., the EU's General Data Protection Regulation versus the California Consumer Privacy Act). Further, depending on the nature of the data, different regulatory frameworks may apply (e.g., in the United States, Health Insurance Portability and Accountability Act of 1996, the Children's Online Privacy Protection Rule, or the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act.

[6] Review should determine whether the existing privacy policy contemplates sharing personal information in the event of a corporate transaction.

[7] See, e.g., Equifax Breach exposes 143m; Social Security numbers, birthdates among data taken. The Boston Globe, Sept. 8, 2017, Uber Breach Kept Secret for a Year, Hit 57 Million Accounts. The New York Times, Nov. 22, 2017 and Scope of Target breach expands; Up to 110m customers may be affected, The Boston Globe, Jan. 11, 2014.

[8] See, e.g., A Deluge of Suits Over Connected Devices Could Be Coming. Law360, Aug. 24, 2018.