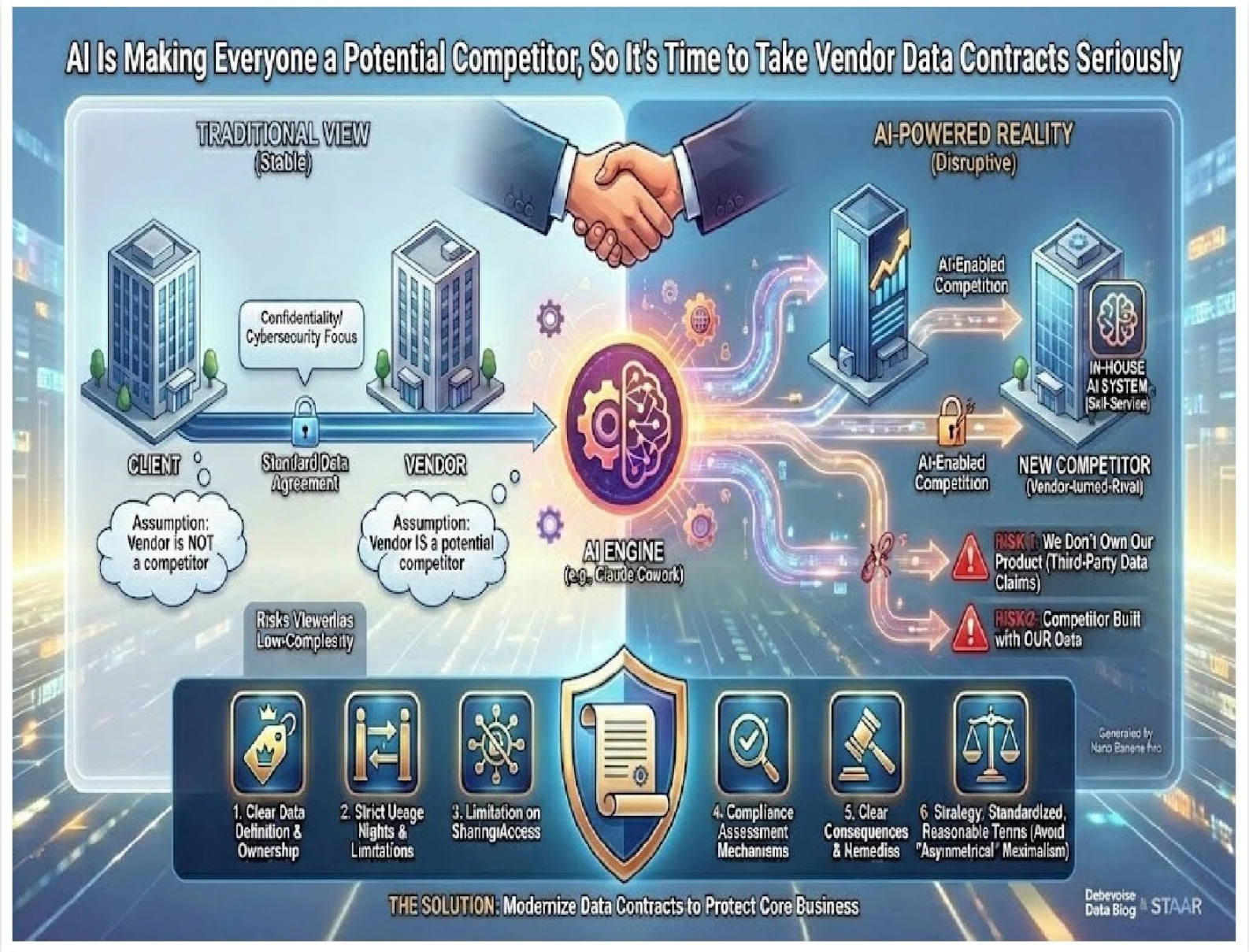
Debevoise & Plimpton | Data Blog

ARTIFICIAL INTELLIGENCE

AI Is Making Everyone a Potential Competitor – Are Your Data Contracts Ready?

BY: CHARU A. CHANDRASEKHAR, AVI GESSER, MATT KELLY, ADAM SHANKMAN, WILLIAM SADD AND PATTY (VIRTUAL AI SPECIALIST) - FEBRUARY 16, 2026



SHARE

- AI is disrupting a core assumption for companies entering routine business agreements: that their counterparty is not, and will not become, a direct competitor. Although non-disclosure terms and

data use limitations have long been standard in many business-to-business contracts, compliance with these terms has rarely been a material concern, and enforcement has been reserved only for extreme cases that involve high-value commercially significant IP. But in the age of AI, many companies are now having to reassess their Data Agreements through a strategic lens, with an eye toward preserving their proprietary expertise and competitive advantage.

Traditional Data Agreement Considerations

Most businesses depend on access to confidential data, which often flows from clients to the company, on to vendors and suppliers, and back again in a loop. This data often represents significant competitive value, reflecting years of accumulated business intelligence, client relationships, and operational insights. Who owns that data, and how it can and cannot be used, are issues that are determined by various contracts, licenses, and terms of use, which we refer to as Data Agreements. These Data Agreements are usually drafted by in-house lawyers and negotiated between procurement professionals. Traditionally, these contracts have received little attention from senior management because they are somewhat standardized and the risks addressed (*e.g.*, cybersecurity and confidentiality) were viewed as unlikely to affect the company's competitive position.

AI Capabilities Dramatically Expand the Scope of Potential Competition

For many businesses, that core assumption – that your clients, customers, vendors, suppliers, service providers, platforms, and other third parties that you share confidential data with are not going to use that data to compete with some part of your business – is increasingly under review. AI systems can analyze vast datasets to identify patterns, generate insights, and create new products or services. This means that data shared with a counterparty today could become the foundation for a competing offering tomorrow, even if that counterparty had little historical presence or expertise in your industry.

Take law firms, for example. We've always had to keep in mind that our clients had in-house legal teams that could do some of the work we do for them. But many law firm clients are now engaging sophisticated legal AI vendors to create systems that may be able to replicate parts of law firm work at scale, and those AI vendors may take what they learn from one project and market similar capabilities to other clients. Many law firms also have direct relationships with legal AI vendors who are both important suppliers of products and services, as well as potential competitors.

Of course, most counterparties are not actually interested in this kind of direct competition, so it is important not to overreact. But the fact that some counterparties are exploring new capabilities also means that the risk cannot be ignored, particularly given the speed at which AI capabilities are advancing. In most cases, these developments should not lead businesses to limit the flow of data to these counterparties, which can be detrimental to the business. Instead, companies should look at their core data sharing relationships and the corresponding Data Agreements to ensure that (i) they accurately reflect the intended business arrangement, (ii) the company is still receiving the benefit of the bargain, and (iii) they provide adequate protection against emerging competitive risks.

What Happens If You Ignore This Issue?

For the companies that ignore this issue, we have seen two significant business risks.

1. *Devalued Products and Services*

Many companies are building AI-enabled products or services using confidential data, including data received from third parties. If those third parties can credibly claim that they own the data, and that the company did not have the rights to use it for such purposes, they may be able to extract significant additional value based on their potential data rights or even prevent the use and sale of the products or services.

2. *Competition from Products or Services Built Using Company Data*

For companies that share confidential data, if there are not sufficient limitations in the relevant Data Agreements, counterparties take the data they receive for the purpose of providing a narrow service to the company, and use it to (i) reduce their need for traditional R&D, and (ii) accelerate the development of something that competes with the company.

Contract Terms to Protect Core Businesses

To reduce these risks, there are several terms to consider for contracts with key data partners:

The scope of Company data;

Allocation of ownership rights over Company data;

Usage rights and limitations for Company data;

Prohibitions on sharing Company data;

Role-based restrictions on who can access the data;

Storage and retention conditions during the life of the agreement;

Destruction or return of Company data upon termination;

Ways to assess compliance;

Consequences and remedies for violations.

While bespoke high-level negotiations may be required for certain key data counterparties, most third-party contracts can be standardized so as not to render your vendor procurement and renewal process unworkable. It is important to have reasonable expectations as to what can be accomplished. Many companies mistakenly try to achieve asymmetrical data rights – no one can use AI with their data without express consent, but they can use AI on everyone else's data without restriction. While this may work for the rare engagements that are inherently asymmetric, this is obviously an unworkable framework to achieve at scale. Worse still, it can lead to wasted time negotiating for maximalist legal positions that, even if accepted, are unlikely to be complied with or enforced, and are not necessary for achieving business goals in most cases. In most instances, a more effective approach is to focus on the specific competitive risks that matter most to your business and negotiate targeted protections that address those concerns. Either way, companies should consider how to manage the risks arising from procurement professionals making strategic

business decisions when negotiating Data Agreements without well-considered guidance and training.

To subscribe to the Debevoise Data Blog, please click here.

The Debevoise STAAR (Suite of Tools for Assessing AI Risk) is a monthly subscription service that provides Debevoise clients with an online suite of tools to help them with their AI adoption. Please contact us at STAARinfo@debevoise.com for more information.

The cover art for this blog was generated by Nano Banana Pro.

Charu A. Chandrasekhar

Charu A. Chandrasekhar is a litigation partner based in the New York office and a member of the firm's White Collar & Regulatory Defense and Data Strategy & Security Groups. Her practice focuses on securities enforcement and government investigations defense and artificial intelligence and cybersecurity regulatory counseling and defense. Charu can be reached at cchandra@debevoise.com.

Avi Gesser

Avi Gesser is Co-Chair of the Debevoise Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He can be reached at agesser@debevoise.com.

Matt Kelly

Matthew Kelly is a litigation counsel based in the firm's New York office and a member of the Data Strategy & Security Group. His practice focuses on advising the firm's growing number of clients on matters related to AI governance, compliance and risk management, and on data privacy. He can be reached at makelly@debevoise.com

Adam Shankman

Adam Shankman is an associate in the Litigation Department. He can be reached at adshankm@debevoise.com.

William Sadd

William Sadd is the Head of Practice and AI Systems at Debevoise. He can be reached at wjsadd@debevoise.com.

Patty (Virtual AI Specialist)

Patty is a virtual AI specialist in the Debevoise Data Strategy and Security Group. She was created on May 3, 2025, using OpenAI's o3 model.

PREV POST

Avi Gesser Recognized in Chambers Global Market Leaders Rankings for Artificial Intelligence

- 2 MINS READ

NEXT POST

Update: Judge Rakoff Issues Written Opinion that AI-Generated Documents Are Not Protected by Privilege

- 7 MINS READ

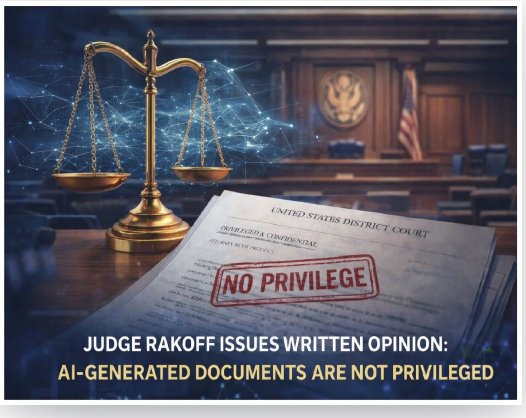
Related Posts

Debevoise Featured in Law360 Story on Vibe Coding

FEBRUARY 24, 2026

Why Companies Should Consider Requiring Internal Disclosure of AI Use

FEBRUARY 22, 2026



Update: Judge Rakoff Issues Written Opinion that AI-Generated Documents Are Not Protected by Privilege

FEBRUARY 17, 2026

Top