# The Top Eight AI Adoption Failures and How to Avoid Them

**June 15, 2023**

Over the past three years, we have observed many companies in a wide range of sectors adopt Artificial Intelligence ("AI") applications for a host of promising use cases. In some instances, however, those efforts have ended up being less valuable than anticipated—and in a few cases, were abandoned altogether—because certain risks associated with adopting AI were not properly considered or addressed before or during implementation. These risks include issues related to cybersecurity, privacy, contracting, intellectual property, data quality, business continuity, disclosure, and fairness.

In this Debevoise Data Blog post, we examine how the manifestation of these risks can lead to AI adoption "failure" and identify ways companies can mitigate these risks to achieve their goals when implementing AI applications.

**Cybersecurity (Data Storage and Untested Plug-Ins)**. To support AI training and use, companies often take large volumes of sensitive company or client data from a secure location and aggregate them in a data lake or data warehouse. If these new locations are not properly secured, the underlying data becomes vulnerable to attack and theft. Many companies that are new to cloud storage, for example, lack experience with all the necessary security configurations to ensure that the data is protected from such threats. In addition, while there are many benefits of using AI applications that are provided by third parties, those that come in the form of browser plug-ins or extensions may expose company network environments to a third party's undetected vulnerability. Similarly, companies may provide an insecure third-party vendor access to sensitive data as inputs or training data for development of an AI solution.

- ***Mitigations***: Information security personnel should be involved in planning and implementing big data and AI projects to secure data storage locations. Consider using internal or outside penetration testers to ensure that any repository used to house data to support an AI initiative is subject to appropriate risk-based security testing and hardening. Also consider limiting the ability of employees to download or install applications or browser extensions unless they have been fully vetted by the company's information security team. Conduct cybersecurity diligence on AI providers to ensure that they can be trusted with sensitive company data, or provide

them with only non-sensitive sample data, synthetic data, or data that has been pseudonymized, anonymized, or tokenized. In addition, consider having the vendors delete confidential company data as soon as practicable.

**Privacy (Sharing Personal Information and Biometrics)**. Many AI projects involve large volumes of personal information of either employees or customers. Using personal information for training or building an AI application, and sharing that information with third parties, who may be involved in developing the applications, can violate privacy regulations. These projects may also involve the use of faceprints, voiceprints, or other digital files that are linked to specific persons, and therefore are subject to privacy and other laws that specifically regulate the use of biometrics.

- ***Mitigations***: Ensure that all the necessary privacy notices and consents are in place, or consider pseudonymizing, anonymizing, or tokenizing the data to reduce privacy risks. Where possible, avoid using biometrics if simpler methods are as effective.

**Contracts (Limitations on Use, Sharing, or Performance)**. Similar to privacy risks, many AI projects involve large volumes of client or other third-party data that are subject to contractual confidentiality restrictions that limit the ability of the company to share that data with third parties involved in implementing the AI applications. There may also be use limitations that constrain the company's ability to utilize that data for testing or training an AI application, as well as other contractual terms relating to means-of-performance, supervision, transparency, quality, and subcontracting, which may limit the company's ability to use the data as part of an AI project.

- ***Mitigations***: Review existing contractual agreements to understand how data may be used and, where there are limitations, consider obtaining written consent from clients to use their data for a particular AI project. Going forward, consider updating contractual agreements to make clear when data may be used to develop AI applications.

**Copyright and Intellectual Property Rights**. Similar to incurring contractual risks, companies sometimes use data to train or operate their models that are subject to copyright protections or licensing terms that restrict permitted uses of the data, which can put the use of the models at risk. Additionally, where companies use models to generate new content, they may have difficulty claiming intellectual property rights and associated protections on those outputs under various circumstances. The United States Copyright Office's current position is that copyright only protects material that is the product of human creativity and AI-generated content must be disclaimed on registration applications. A Fair Use defense may apply to a copyright infringement claim, but such arguments are still relatively untested and highly fact-dependent.

- ***Mitigation***: Consider negotiating for permission to use the copyrighted materials. Going forward, consider revising contractual agreements with counterparties to provide express rights to use their data to train or operate the company's AI models under commercially reasonable conditions (e.g., the data is not transmitted or made available to third parties, models trained on protected data are for internal use only, the models will not be used to try and replicate or replace the copyrighted data, etc.). If copyright registration is contemplated, consider taking steps to evidence the degree of human contribution to the AI-assisted generation of creative works.

**Data Quality**. Companies may train AI models on data that is not comprehensive or is not fully representative or relevant to the circumstances in which the models are being used. For instance, in the midst of the COVID-19 pandemic, many AI models that had been trained on historical pricing data failed because they were unable to account for market changes.

- ***Mitigation***: Consider stress testing models with novel or low-probability/high-impact scenarios to see how they would behave if market conditions were to change unexpectedly. Also consider implementing guardrails so that model operators are alerted to significant changes in model inputs or outputs, and models can be recalibrated quickly following any significant unexpected changes.

**Business Continuity**. Many AI applications contribute significantly to essential business functions, which can lead to business continuity risks if the applications need to be taken offline for maintenance, to investigate potential problems, or because of other operational or legal concerns.

- ***Mitigation***: Consider running certain high-risk AI applications in a sandbox or alongside a more traditional or proven method for achieving its results for some period before full deployment to ensure that the AI application is working as anticipated. Consider maintaining earlier versions of the model or other models that can be put into operation if the model must be taken offline, as well as other ways to accomplish the task being conducted by the model to ensure business continuity.

**Accurate Disclosures**. Companies have suffered regulatory and reputational harm for misleading clients into thinking that decisions are being made by humans when, in fact, they are being made by algorithms. For example, the SEC has previously brought an enforcement action against an investment advisor that allegedly replaced live traders with algorithmic trading strategies, while hiding those changes from fund investors. Similarly, companies that exaggerate the capabilities of their AI applications may face scrutiny from the FTC and other regulators.

Mitigation: Consider providing targeted training for marketing and compliance teams on the risks of misstating the use of AI. Ensure that language in marketing materials referencing the use of AI is reviewed by internal AI subject-matter experts for approval prior to dissemination.

**Fairness**. Existing anti-discrimination laws, as well as new laws specifically applicable to AI, can place limitations on how AI can be used for certain decisions that impact individuals' rights and opportunities, including hiring, lending, and insurance underwriting. For example, if an AI application that is designed to screen resumes is configured to penalize job candidates who have a gap of a year or more on their resume, that could create regulatory and reputational risk if it has the effect of screening out a significant portion of older women applicants who took time off to raise children.

- ***Mitigation***: Consider examining the inputs of AI models involved in important decisions for individuals to ensure that they are appropriate considerations for the relevant decision and are not proxies for protected classes like race, gender, or ethnicity. If it is unclear why a particular input is predictive, consider testing that input for bias or removing it from the model.

To subscribe to our Data Blog, please click here.

*The Debevoise Artificial Intelligence Regulatory Tracker ("DART") is now available for clients to help them quickly assess and comply with their current and anticipated AI-related legal obligations, including municipal, state, federal, and international requirements.*

*The cover art used in this blog post was generated by DALL-E.*

* * *

Please do not hesitate to contact us with any questions.

**NEW YORK**

Avi Gesser
agesser@debevoise.com

Matt Kelly
makelly@debevoise.com

Samuel J. Allaman
sjallaman@debevoise.com

Michelle H. Bao
mbao@debevoise.com

Anna R. Gressel
argressel@debevoise.com

Michael Pizzi
mpizzi@debevoise.com

Lex Gaillard
adgaillad@debevoise.com

Cameron Sharp
cdsharp@debevoise.com

**WAGHINGTON, D.C.**

Esther Tetruashvily
etetruashvily@debevoise.com