



# A Framework for Due Diligence of Data in an M&A Transaction

05.21.2019

The broad adoption of technologies that collect, analyze, store and distribute data is disrupting a number of industries. It is also proving to be a challenge for lawyers attempting to apply existing laws and regulations to the novel issues these technologies raise. One area of law that is often overlooked is conducting due diligence of a target company's data assets in a corporate transaction, since data have become critical corporate assets for a number of businesses. As it does with the other corporate assets of a target company, the acquiring company must ensure that any risks associated with these data assets have been identified and, to the extent possible, mitigated. In addition, the acquiring company should ensure that the value of the target company's data assets is adequately protected.

The first three posts in this series have highlighted several challenges lawyers will face when conducting due diligence of data assets, including:

- The law associated with data is often unclear and evolving;
- Innovative new uses for data are being developed;
- The target company may not know the extent of its own data assets or how they are used; and,
- Due diligence must cut across both technology platforms and legal domains.

They have also described key due diligence issues that an acquiring company should consider with respect to the target company's data assets.

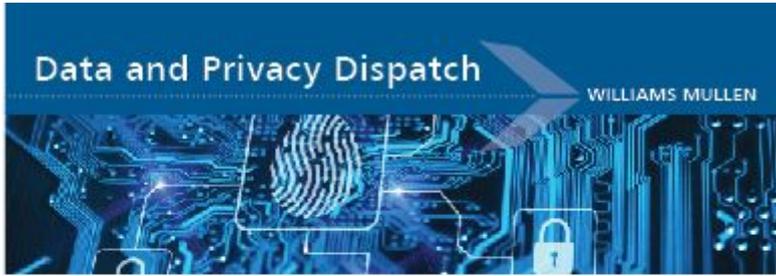
- [Data Due Diligence in M&A Transactions: Data Protection/Privacy](#) – This post discussed due diligence in connection with privacy/data protection issues. This type of due diligence has become increasingly important after reports of several high-profile data breaches of target companies that occurred before acquisition. The post explained why it is critical for the acquiring company's counsel to identify what personal data the target company has collected and how the data were acquired, used and stored in order to ensure compliance with applicable laws, policies and agreements. Due diligence should also be conducted on the target company's cybersecurity

practices and policies.

- [Data Due Diligence in M&A Transactions: Ownership Rights in Data](#) – The second post focused on the importance of understanding ownership rights in data. Unfortunately, as the post discussed, ownership rights in data are not as clear as with many other types of assets. It explained that there are two primary considerations when conducting due diligence on the target company's rights in its data assets. First, the acquirer needs to determine whether the target company is adequately protecting rights it may have in its own data. Second, the acquirer must ensure that the target company's is not violating any third-party rights.
- [Data Due Diligence in M&A Transactions: Data Quality and Liability](#) – The most recent post examined due diligence for potential liability risks associated with data quality. This type of due diligence is becoming more critical as important decisions are made in near real-time based upon data collected from technologies such as the Internet of Things (IoT). In addition, as businesses integrate machine learning and artificial intelligence (AI) into their operations, much of the data often will be collected, processed and used without significant oversight by humans, making data quality issues even more difficult.

### **[Five Key Areas for Framework Development](#)**

Please [click here](#) to view five key areas of focus when developing a framework for conducting due diligence of data assets in a corporate transaction.



## A Framework for Due Diligence of Data in an M&A Transaction

Five key areas of focus when developing a framework for conducting due diligence of data assets in a corporate transaction:

### OPERATIONAL CONSIDERATIONS

There are several operational matters related to data that should be considered. These include:

- > What types of data does the company collect itself?
- > What types of data does the company obtain from third parties?
- > What data does the company transfer to third parties?
- > How does the company use and store its data?
- > Where is the data stored?
- > Are the appropriate laws and policies being followed for personal information?
- > Who has access to the data?
- > What cybersecurity measures has the company implemented?
- > Has the target company been sued, or threatened with litigation or an enforcement action, for failing to protect personal information or for otherwise violating an individual's privacy?
- > Are the data "fit for purpose" for all the applications for which they are being used?

### OWNERSHIP RIGHTS

Understanding ownership rights in data, and products and services created from data, is particularly challenging. However, some of the key considerations include:

- > Does the company create data products and services that are shared externally?
- > Does the company use data from third parties to create products or services for either internal or external use?
- > Is the target company using open data that are subject to share-alike licenses?
- > What rights does the target company have in derivative products created by aggregating third party data with the company's data?
- > Are employees "scraping" data from third party websites?

### INTERNAL POLICIES AND PROCEDURES

As with other critical issues, it is important to understand the target company's policies and procedures regarding its data, including:

- > Internal data protection and privacy policies;
- > Information security and cybersecurity plans;
- > Employee training;
- > Data breach response plans;
- > Business continuity plans; and,
- > Data Quality Assurance/Quality Control (QA/QC) policies and procedures.



## Related People

- Kevin D. Pomfret – 703.760.5204 – [kpomfret@williamsullen.com](mailto:kpomfret@williamsullen.com)