Data Due Diligence In M&A Transactions: Ownership Rights in Data

04.04.2019

As data are quickly becoming a significant corporate asset, lawyers in corporate transactions need to consider the legal risks associated with data. Failure to understand and address these risks can result in significant future costs to the acquiring company. There are a number of due diligence considerations for a potential buyer with respect to data assets. The first post in this series discussed due diligence in connection with privacy/data protection issues. This post will examine due diligence of a target company's rights in its data assets.

There are two primary considerations when conducting due diligence on the target company's rights in its data assets. First, whether the target company is adequately protecting rights it may have in its own data. The second is to make sure that the target company's use of data is not violating the rights that third parties may assert in their data.

Protection of Rights in Data

Unfortunately, intellectual property rights in data are not as clear as with many other types of intangible assets, such as software. For example, in the U.S. factual data – such as directories, or places of interest – generally only receive "thin copyright" protection.[1] That is, the data themselves are not protected by copyright, but how the data are organized or structured might be protected. In other jurisdictions, such as in the European Union, there is legislation that specifically protects intellectual property rights in data bases.[2] However, this legislation is subject to much uncertainty as well.

If the target company is using data solely for internal purposes, the primary question from a due diligence question is whether it has worked with third parties to collect, process or analyze the data. For example, the target company might have hired a vendor to track its mobile assets using GPS-enabled devices. Alternatively, it may have hired a company to analyze customer movements through its retail stores. Each of these scenarios raises data protection and privacy issues. However, it is also important to review the agreements to determine what rights the target company has granted in the original data and whether it has sufficient rights to use the processed data. It will also be important to understand what rights (contractual or otherwise) the target company has in any products or services that may have been derived from the original data.

If the company creates data products and services that are shared externally, it is important to understand what methods the target company has in place to protect its rights in the data. (Such products and services would include a simple map or visualization tool, an augmented

reality app or a machine learning algorithm.) The protections might be technological – i.e., the data are published in a form that is difficult to copy or – legal through copyright, if applicable, trade secrets or contract.

Third-Party Rights in Data Assets

Understanding a target company's right in its data assets becomes even more complex as companies use data from third parties to create products and services. Particularly if they aggregate third-party data with their own data. This third-party data generally will be subject to licenses that can contain a number of restrictions. In conducting due diligence it is important to confirm that the rights the target company is giving its customers in the data included in a product or service conform with the original license from the vendor.

In some instances, this third-party data will be licensed under "open data" licenses. Open data licenses are similar to open source software licenses. However, there is much less uniformity associated with open data licenses than with software licenses. Therefore, these licenses can vary greatly with respect to matters such as attribution, share-alive provisions and whether commercial use is permitted. If a target company is using open data, it is important to confirm it has complied with the applicable open data license. It is also important to make sure that the target company's open data do not unintentionally taint the acquiring company's proprietary data through unwelcome share-alike provisions.

Another challenge is ensuring that the target company has the necessary rights in any derivative products have been created by aggregating third-party data with the company's data. The question of what constitutes a derived product from a data standpoint is challenging, as data products can include data from a number of sources, each subject to its own license agreement. It can be even more difficult if, as is often the case, the matter is not clearly spelled out in the agreement between the parties.

Another due diligence challenge to consider is that some employees of the target company, due to the uncertainty associated with intellectual property rights in data, may have believed it was permissible to "scrape" data from third party websites. The appropriateness of this method to collect data is an open issue, as there are a number of potential legal challenges to protect against web scraping in addition to intellectual property rights[3]. For example, courts are being asked to consider whether scraping violates a website's terms of service, or whether computer fraud statutes may apply.

Understanding rights in data is becoming increasingly critical as more types of data are being collected and used from nontraditional sources, using new sensors and technologies. For example, questions are arising as to who has rights in data collected about a passenger in an autonomous vehicle: the automobile manufacturer, the individual or a third party that provides services using the data? Alternatively, are data collected by a sensor in a home owned by the homeowner, the device manufacturer or the software provider? Until lawmakers change the existing framework, the answers are currently being addressed primarily by contract. As a result, it is important for the acquiring company to understand what rights and responsibilities it has in the data that it is acquiring.

[1] Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991) https://www.law.cornell.edu/copyright/cases/499_US_340.htm .

[2] Directive 96/9 EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[3] See e.g. Craigslist Inc. v. 3Taps., 942 F.Supp.2d 962 (N.D. Cal. August 16, 2013); hiQ Labs, Inc. v. LinkedIn, Corporation 273 F.Supp.3d 1099 (N.D. Cal. Aug 14, 2017).

Related People

- Kevin D. Pomfret – 703.760.5204 – kpomfret@williamsmullen.com