THE M&A JOURNAL

THE INDEPENDENT REPORT ON DEALS AND DEALMAKERS

VOLUME 18 NUMBER 7

Stephanie Sharron

Erin Bosman

Khoa Do

Christine Lyon

Five Key Legal Risks for Data-Centric Technology M&A

By Stephanie Sharron, Erin Bosman, Khoa Do, and Christine Lyon of Morrison & Foerster

Data, and the associated technology platforms that analyze and process data, play a vital role in today's M&A transactions. Not only is the data itself often a core asset that is a key factor in driving M&A valuations, but the platforms and tools that process data raise business-critical risks that may impact the acquiring company's core businesses in unexpected ways.

These risks are heightened for companies whose products and services may unintentionally give rise to real world harms, whether they are part of the Internet of Things (IoT), autonomous systems such as autonomous vehicles and industrial machinery, wearables and digital health devices, fintech products and services, or the data analytics, artificial intelligence (AI), and machine learning tools and platforms that support them.

Across industry sectors, issues concerning data rights, intellectual property rights, product liability, regulatory compliance, and cybersecurity are paramount. While awareness of privacy vulnerabilities and cybersecurity threats is increasing, with news headlines dominated by high-profile data security incidents, risks associated with weak or absent data rights and other risks are less well understood. And though eliminating all risks often is not practical, risks can be expertly managed.

Through effective due diligence practices, legal counsel can help companies identify the role of data in the business, its value within the target company, and the risks associated with that data.

Valuations of target companies can be impacted by the value of the data access and use rights. Moreover, significant regulatory risk and exposure can arise if a company does not properly manage its collection, usage, and sharing of this data, as well as how the company secures the data it processes and stores. Understanding both the data that a company processes, and how it is used and shared, is of growing importance in M&A due diligence.

Below are five key questions to consider in these M&A transactions:

1. Does the company have adequate rights in core data assets?

An important function of the due diligence is to assess whether the company has secured adequate rights to collect, process, and share the data that it uses. Focus and prioritization are essential to approaching these issues efficiently. Before diving into the minutiae of mapping data flows, for example, first determine what data is core to the target company's business value,

Legal Risks ➔

Legal Risks

continued

as well as what data might attract the greatest regulatory scrutiny. Then, assess whether the target company has taken adequate precautions to protect that value and address those compliance risks. Finally, look for areas where a target company's inattention to a key risk could impact the acquiring company's core business. When assessing rights in data, a useful approach is to separate the regulatory compliance concerns from the rights in data from an intellectual property and common law perspective.

Beginning with compliance, when a targeted company's business relies on processing personal data and in particular, when personal data is a core asset of the target company, the due diligence inquiries should be focused on whether the target company has implemented adequate procedures to ensure that processing of personal data complies with applicable law. Typically, these obligations include notice to and, in some instances, consent from individuals whose personal data is processed, depending on the type and sensitivity of such data, as well as to whom it pertains and how it is collected and further processed.

What constitutes adequate notice, and when consent is required, may differ from jurisdiction to jurisdiction. In general, the more sensitive the data and the more surprising the planned use of it, the greater the obligation to inform and obtain consent of the individual. The details matter when processing personal data. In regulated industries, such as health care, financial services, and telecommunications, or when dealing with the personal data relating to children, the U.S. laws are far more prescriptive. Outside the United States, more control tends to be wielded by the individual with respect to the use and further sharing and processing of personal data. And even the precise definition of personal data differs widely around the world.

Privacy statements, policies, and notices (both internal to the company and external) are one common tool for navigating these privacy law requirements. Put simply, due diligence can help assess whether the target company has procedures in place to ensure that it accurately "says what it does" and "does what it says" in these internal- and external-facing documents. Privacy requirements go well beyond the privacy policy, however. Data protection laws—most notably, the new EU General Data Protection Regulation, with its potential penalties up to the greater of 20 million Euro or 4% of total worldwide annual turnover for the prior financial year—require careful attention to privacy throughout the data life cycle. New requirements for "privacy by design" are accompanied by greater regulation of profiling, tracking, and automated decision-making, all going straight to the heart of many artificial intelligence, analytics, and targeted advertising technologies. While the legal risks of noncompliance are substantial, the business risks are even greater: companies that fail to build privacy compliance into their data-centric technologies may set themselves up for failure in a marketplace of increasingly sophisticated consumers and enterprise customers. Similarly, a buyer that acquires such a company may discover that the privacy-related deficiencies cannot be easily remediated post-closing, and that it may be necessary to invest even more time and resources in fixing or even rebuilding the data-centric technology it has acquired.

Even if data privacy issues have been adequately addressed, the company still may not have sufficient rights to process data in the manner in which it currently operates or intends to operate. Assessing whether a company has taken adequate precautions to secure the necessary rights beyond data privacy compliance involves a combination of focused inquiries about the target company's practices, a review of contractual commitments and data policies, and an understanding of relevant law.

A variety of legal theories may support claims that a third party's rights have been abridged when even non-personal data is collected and processed without adequate precautions. These include, by way of example, computer fraud, misappropriation, unfair competition or deceptive practice, trespass, negligence, conversion, and claims under the Stored Communications Act and the Wiretap Act.

Data collected from business partners or customers, for example, may be considered trade secrets depending on context or might constitute confidential information under confidentiality and non-disclosure agreements that restrict use of the data. Alternatively, those whose systems are accessed may claim that a target company's collection of data in connection with its product or service was conducted in an unauthorized manner or that the underlying data constitutes their property and not the target company's property. The risk of claims is greater in the absence of transparency and disclosure about the target company's practices, especially when

harm or injury to a person or entity is apparent. And of course, contracts with suppliers as well as customers can also restrict how data is accessed and used, creating tripwires for companies that do not align their business practices with their contracting practices.

The structure of an M&A transaction may also impact rights in data. In a reverse triangular merger where the target company survives, for example, the impact on the target company's post-closing rights in the data may not be impacted even in the absence of express rights from data providers to assign or transfer data because, in fact, there has been no assignment or transfer. However, in a forward merger where the target company merges into the acquirer, or if the transaction is structured as an asset sale, rights in data may not survive. Moreover, when the target company initially survives and there is no immediate assignment or transfer, but the acquiring company opts to later roll up the target company into itself or into another company, rights in data may be adversely impacted. Thus, acquirers often will want to conduct due diligence to confirm that data assets can be transitioned and the rights associated with them will transfer without an adverse change in terms. If personal data is involved, then privacy statements and policies should be reviewed to confirm that they provide for rights to transfer data on an acquisition, merger, or other change in control of the target company.

In summary, when insufficient attention to regulatory compliance issues or data rights issues may impact the core value of a target company, or create substantial liability for the acquiring company, a deeper dive in due diligence is always prudent.

Takeaways:

- Assess whether the target company has secured adequate rights to the data it processes both from a regulatory and a non-regulatory perspective. Be sure to understand not only the target company's current pursuits, but also any future activities that form the basis of its valuation.

- Determine whether data that will be transferred to or used by the acquirer is subject to any extra-contractual limitations on such transfer or use that might constrain the anticipated value to the acquirer's business or otherwise pose unexpected challenges for the acquirer.

- Review agreements with third parties that may restrict transfer or use.

- Evaluate what regulatory compliance obligations apply to the collection, processing, and sharing of data (including those of foreign jurisdictions) and assess whether the company has a procedure in place to assure compliance. Determine whether any complaints have been filed, or whether any regulatory actions have been asserted, against the company.

- Review the company's privacy practices and procedures, including the design of its data-centric technologies, and confirm that the practices disclosed by the company in its external-facing policies and notices match the company's actual practices.

- Establish reasonably protective representations and warranties in the purchase agreement and, where appropriate, negotiate special indemnities to address particular risks of heightened concern. Consider having privacy and data security representations included as fundamental representations that are subject to indemnification (up to amount of a pre-defined escrow) and that survive for a designated period of time (similar to how intellectual property infringement risk is commonly addressed).

2. What other intellectual property risks does the company face?

Many highly valued target companies with data-centric technology companies focus on building data analytics platforms and tools that are based on algorithms developed and refined over time. When such algorithms are developed and data models are trained using data made available by third parties, it is important for the acquiring company to ensure that the target company has the rights to use the data for this purpose in the first place. Evaluating whether these rights existed in the past and will continue into the future depends on the type of inquiry and diligence described in Section 1 above, as applied to these development activities.

For the IoT and other connected products and services, perhaps more than in other areas of technology, patent infringement risk is another significant area of potential concern. Because many

Legal Risks ➔

Legal Risks

continued

layers of the technology stack are employed in these connected ecosystems, the risk of patent infringement is heightened. These technology layers, including many of the same network and communications technologies and protocols central to connected device functionality, have been the subject of intense patent protection. Many of the largest holders of patent portfolios in the technology space play a central role in how these patents are licensed and asserted against alleged infringers.

Adoption of technical standards is one approach companies are expected to pursue, not only to help mitigate infringement risk, but also to facilitate interoperability between disparate systems. These standards offer varying levels of protection against patent infringement claims by others following the same approach.

Here's how it works at a high level. By participating in standards setting organizations, a member often obtains a license under other members' patent claims that are necessarily infringed by implementation of mandatory portions of the specifications promulgated by the standards body. In exchange, the member agrees to license its patents on the same terms. The specific terms of the license will vary, and some may require royalties.

Although standards can help mitigate infringement risk in certain instances, acquirers must evaluate the impact of these standards licenses on their own patent portfolios, especially when the acquirer intends to roll up the target company into itself. Since potential infringement risks may still exist with elements of the target company's technology, products, and services that fall outside of the mandatory portions of the standard, acquirers should be aware of, and consider whether to perform, a freedom-to-operate analysis on key aspects of the target company's products or services.

A final intellectual property issue of particular relevance in this area of M&A is participation in open source projects. Such participation is becoming increasingly common for companies that develop products and technologies in the fields of AI, machine learning, and IoT. In addition to customary open source software due diligence, an acquirer would be prudent to dig deeper into whether the target company's engineering talent engages with and makes contributions to open source projects.

This due diligence can be of significance to acquirers because, by contributing to open source projects, target companies can inadvertently grant implied or express licenses under patents. Moreover, since these licenses may extend to a company's affiliates (including parent entities), post-acquisition participation and contributions could impact the acquiring company's own patent portfolio and how it is licensed. Understanding the potential scope of such commitments is therefore important to understanding more commonly considered concerns about a company's ability to protect the proprietary nature of its software, as well as the implications for the target company and the acquiring company's patent portfolio. When applicable, due diligence therefore should include review of the contributor agreements pursuant to which those contributions have been made.

Other intellectual property risks not dissimilar to those generally faced by technology companies also apply to data-centric M&A transactions, so customary intellectual property due diligence is also recommended.

Key questions:

- Have any claims of infringement of intellectual property or other rights of third parties been threatened or asserted?
- What steps has the company taken to mitigate against the risk of intellectual property infringement claims?
- Has the company received any threats or letters of inquiry related to licensing of third-party patents?
- Has the company obtained any patent non-infringement opinions? If so, with the assistance of counsel, further inquiry into the substance of such opinions as well as the context of why they were obtained may be prudent.
- Of which standards setting organizations is the company a member? Evaluate any intellectual property licenses that apply to the company in connection with the company's participation in such standards.
- In addition to customary due diligence relating to open source software use, ask with which open source projects the target company's employees and consultants may be

working and to which they may be contributing code. Review contributor agreements for each such project.

3. Has the company adequately managed cybersecurity risks?

Most companies today are considering how to integrate cybersecurity preparedness into their processes. When data is one of the key assets of a target company, or is essential to the development and operation of its products or services, these issues are not just a matter of prudence; they also influence the core purpose of the acquisition. Thus, it is all the more important to understand whether the target has responded effectively to past cybersecurity threats and is well-prepared to respond in the future.

In the context of M&A due diligence, this translates into assessing whether a target company's data security practices correlate well with the sensitivity and value of the data processed. When assessing risk with respect to an M&A transaction, determine whether the target company has experienced any data security incidents resulting in the exposure of confidential information, personal information, or safety and security risks, and what, if any, protective measures the target company has taken. Also vital to mitigating cybersecurity risk is whether the target company has put in place an effective incident response plan.

Takeaways:

- Ensure that security experts conduct technical diligence on key systems and processes of the target company to assess whether and what sort of security vulnerabilities exist in connection with data and network security, physical security, and other security and safety issues.

- Review any prior data breach or other cybersecurity incidents, what data and systems were compromised, and how the target responded, including whether responses complied with applicable regulatory requirements.

- If prior incidents have arisen, assess what existing and future risks and liabilities might be associated with such incidents and craft representations, warranties, and special indemnities to address these concerns.

- Then, review the target company's incident response plan to determine its preparedness to respond to a data breach, cyberattack, or other intrusion in the future.

- Post-closing, take appropriate steps to address weaknesses identified in diligence and to integrate the target company into the acquirer's incident response plan and cybersecurity risk mitigation practices.

4. What is the company's current product liability risk profile and how has the target company mitigated product liability risk?

The reach of data-centric technology beyond just the end user significantly increases the product liability risk profile for M&A transactions. Concerns about potential product liability arise out of use of autonomous vehicles and other autonomous systems, wearables, digital health, the IoT, and fintech. Potential claims of personal injury or property damage are easy to imagine, whether due to alleged manufacturing defects, design defects, or because of a security hack. Many have experienced or speculated on the potential harm of the hacked digital lock, the smart thermostat that goes into overdrive and overheats a home, or the smart smoke detector that doesn't detect. Now we are beginning to see the real world complexity of allocating risk with respect to autonomous systems such as cars and other transportation systems. Transacting virtual currency over distributed ledgers and automated trading in the financial services space has given rise to extraordinary losses in some cases. With each advance in data-centric technology, product liability risks and a mitigation strategy must be evaluated and implemented.

In light of the elevated potential for losses and product liability exposure, when engaging in M&A activity that involves data-centric connected systems, acquirers need to take additional steps to assess the target company's product liability risk profile and what steps the target company has taken to mitigate that risk. Some key questions that will help an acquirer assess product liability risk include:

- Has the target company been sued by individuals claiming bodily injury or property damage? Has the use or commercialization of the target company's products or services resulted in any claims of bodily injury or property damage?

Legal Risks ➔

Legal Risks

continued

- Have any privacy or security breaches resulted in claims or bodily injury or property damage?

- What policies and procedures does the company have in place to track product safety issues and determine whether a potential hazard exists?

- Has the target company managed risk in negotiating contracts with both suppliers and customers? Has the target company obtained contractual protections against third-party claims for risks beyond the target company's reasonable control?

- For products and services involving heightened risk, what notices and warnings has the target company employed and how have they been delivered to the customer?

- Has the company adequately informed consumers of their own duty to maximize cybersecurity?

- Assess insurance the target company has procured and the adequacy of its insurance contracts.

- Particularly when a target company is engaged in a business where product liability risk is heightened, review the company's insurance policies as well as its general contracting practices to assess whether agreements were negotiated to mitigate potential product liability risk.

5. What are the life cycle issues and risks for IoT and other data-centric technology systems?

In IoT and other autonomous and connected systems, it is important to understand how a target company has (or has not) managed the "life-cycle" of transfer of ownership and decommissioning of these systems. The IoT is comprised of many networks of connected sensors that collect, process, and transmit data to and from all kinds of devices. Once these networks of sensors have been installed and turned on, it can be difficult to deactivate them without impacting customers adversely. Consider the connected car or the home appliance that changes hands with the sale of the car or the property. By inquiring about these life cycle issues, acquirers can gain a better understanding of the target company's ability to enable customers to transition products and services to others, as well as the target company's own ability to manage end-of-life products or services over time.

Prepare for Data-Centric Technology M&A Success

M&A transactions that involve valuable data sets, and the application of artificial intelligence, machine learning, IoT, and other data-centric technologies, take place in an exciting and developing realm of economic activity. While there is much reward for those who conduct adequate due diligence and negotiate protections into the purchase agreement before consummating any transaction, significant downside risk exists for those who do not. These risks, though, can be proactively mitigated. Focused due diligence and targeted adaptation of representations and warranties to address concerns uncovered in the due diligence process can be instrumental. Negotiating special indemnities to address identified issues of heightened concern, including representations and warranties insurance, can also mitigate exposure. When parties work closely with counsel experienced in the nuances and complexities of data-centric M&A transactions, they maximize opportunities for reaping the rewards that can be gleaned from these exciting new technologies.

~~MA~~

Stephanie Sharron is a partner in Morrison & Foerster's Palo Alto office and a member of the firm's Technology Transactions Group. Ms. Sharron advises clients focused on leveraging data through technology and the related legal issues that apply to their business models in light of the rapid changes in business, technology and law. She can be reached at ssharron@mofo.com.

Erin M. Bosman is a partner in Morrison & Foerster's San Diego and San Francisco offices, and chairs the firm's Product Liability and Counseling Practice Group. Ms. Bosman provides clients comprehensive counsel from product conception to launch and beyond, and represents them in litigation and product recalls. She can be reached at ebosman@mofo.com.

Khoa D. Do is a partner in Morrison &

Foerster's Palo Alto office and a member of the firm's Mergers & Acquisitions Practice Group. Mr. Do's practice focuses on M&A transactions ranging from mid-market to large-scale acquisitions. He can be reached atkdd@mofo.com.

Christine E. Lyon is a partner in Morrison & Foerster's Palo Alto office and a member of the firm's Privacy + Data Security Group. Ms. Lyon advises organizations on cutting-edge issues related to the collection, use, sharing, and safeguarding of data, including personal information of customers and employees. She can be reached at clyon@mofo.com.

THE M&A JOURNAL
the independent report on deals and dealmakers

Editor/Publisher	**John Close**
Design and Production	**John Boudreau**
Senior Writers	**Gay Jervey, R. L. Weiner**
Writing/Research	**Frank Coffee**, **Jeff Gurner**, **Terry Lefton**
Circulation	**Dan Matisa**
Web Production	**John Boudreau**

The M&A Journal, 614 South 4th Street, Suite 319 , Philadelphia, PA 19147