HUNTON& WILLIAMS

Lawyer Insights

February 22, 2016

How to Safeguard Privacy and Data Security in Corporate Transactions

by Lisa J. Sotto and Ryan P. Logan

Published in Corporate Counsel

Personal information about consumers is the lifeblood of many organizations. In the era of big data and increasingly advanced data analytics, companies can use personal information more effectively to target existing and prospective consumers and gain advantages over competitors. Because of the potential value of the information, companies are increasingly focused on privacy and data security issues that arise in the context of mergers, acquisitions, divestitures and related transactions. In many corporate transactions, data is a critical asset that should be addressed as a key deal point. Just as the financial condition of a target company should be carefully analyzed, so too should a company's data protection practices. Unfortunately, too often personal data is transferred without consideration of issues that otherwise might change the pricing of a deal--or kill it altogether.

This article describes the privacy and data security-related legal issues that arise in corporate transactions, and provides a how-to guide on addressing those issues during the various stages of a transaction. Starting with the due diligence process when initially contemplating a merger or acquisition, companies should conduct a thorough investigation to understand the data protection posture of the target entity. The findings from the inquiry will inform the relevant contract provisions in the deal documents. As a general rule, the more unknowns there are when it comes to privacy and data security, the more carefully crafted the deal documents must be to protect the acquiring company against potential pitfalls. If possible, the parties should cooperate to remediate significant issues before closing. If this is not feasible, the acquiring entity should be prepared to quickly address post-closing any significant privacy and data security compliance issues that remain.

Legal Constraints

There are two key legal issues companies must consider when seeking to manage privacy and data security risks in corporate transactions. First, to comply with the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive trade practices, the acquiring entity must keep any privacy promises the target company made to consumers who provided it with their data. In one early privacy enforcement action, the FTC prohibited Gateway Learning Corporation from selling personal information consumers had provided through the company's website while the site's privacy policy indicated the company would not share the information without first obtaining the relevant consumers' explicit consent. After acquiring the data, Gateway changed its privacy policy to permit such sharing. But Gateway failed to notify the consumers who had provided their data prior to the change and did not obtain their express consent to the company's new information practices.

In the acquisition context, the FTC admonished Facebook in connection with its acquisition of WhatsApp, indicating that Facebook would be required to use the personal information of WhatsApp users in accordance with WhatsApp's privacy policy, which was more restrictive than Facebook's policy. To avoid a possible enforcement action in connection with an acquisition, the acquiring company has a choice: it can use consumer personal information in accordance with the privacy promises made to consumers when their information originally was collected, or it can obtain consumers' affirmative consent to use the personal information in a materially different manner.

Second, companies must comply with relevant statutory and regulatory requirements. As an example, the Privacy Rule promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) permits a covered entity (such as a hospital, pharmacy or health plan) to disclose protected health information for its own "health care operations" without first obtaining the authorization of the individuals whose information is disclosed. The HIPAA Privacy Rule defines "health care operations" to include "the sale, transfer, merger, or consolidation of all or part of the covered entity to or with another covered entity, or an entity that will become a covered entity and due diligence related to such activity."

This would permit a pharmacy chain, for example, to transfer to another pharmacy chain the prescription records of individual pharmacy locations it is divesting. It would not permit the divesting pharmacy chain, however, to transfer those same records to a drug manufacturer for the manufacturer's own marketing purposes. In another example, under the Gramm-Leach-Bliley Act's Privacy Rule, a financial institution may disclose the nonpublic personal information of its consumers in connection with a sale, merger or transfer of all or a portion of the business or an operating unit, but only if the disclosure concerns consumers of the relevant business or operating unit. To put it another way, a bank that sells its credit card division to another bank may disclose to the acquiring bank only the information of its credit card customers (and not, for example, its mortgage customers).

Privacy and Data Security Due Diligence

The first, and perhaps most important, step for the acquiring party is to conduct due diligence on the target entity's privacy and data security practices. This may be just as crucial to a deal as understanding the target's financial status because unidentified privacy and data security issues can have a significant impact post-closing. For example, Company A may be motivated to acquire assets of Company B because of its extensive customer lists that contain personal information and insightful nuggets about those customers' purchasing habits. If Company A fails to conduct privacy-related due diligence and does not discover that Company B's privacy policy states that it "will not share customer personal information," Company A may be barred after the closing from accessing or using Company B's customer lists. The effect is that the transaction may be rendered useless. In another example, Company A acquires Company B which uses outdated point-of-sale (POS) terminals with inadequate security. The POS terminals likely need to be replaced immediately after the closing, increasing the integration costs of the acquisition and risking a security breach that could impose significant post-closing liabilities on Company A.

To prevent these types of issues, every company that intends to merge with or acquire another entity should prepare a comprehensive privacy and data security due diligence checklist to provide to the other party. The checklist should (1) ask pointed questions about privacy and data security issues and (2) request that the target provide privacy and security-related materials such as privacy notices and other relevant representations and information security policies. Sample questions could include:

- What consumer and employee personal information does the company collect and maintain?
- For what purposes does the company use the personal information it collects?
- To what categories of third parties does the company disclose the information?
- Where and how does the company store the personal information it obtains?
- What security safeguards are used to protect the information throughout the lifecycle of the data?
- Does the company have dedicated employees who are responsible for data privacy and information security?
- Are these employees adequately resourced?
- Does the company market via text message or email?
- Is the company in material compliance with relevant privacy and data security laws in all the jurisdictions in which it operates?
- Does the company transfer any personal information from one country to another?
- Has the company received any complaints or correspondence, or been the subject of an investigation or audit, regarding privacy or information security from or by relevant regulators, courts, consumers, employees or others?
- Has the company been accused of any violations of privacy or data security laws?
- Has the company suffered any cybersecurity events or information security breaches during the past five years in which personal data or other business confidential information has been compromised?

The answers to these and other similar questions could significantly affect the purchase price by shedding light on the target entity's privacy practices and the entity's potential exposure to privacy or security-related enforcement actions or potential litigation. The due diligence exercise also could affect the timing of a deal as antitrust regulators increasingly are considering control over personal information as a factor in evaluating the competitive effects of a given corporate transaction. FTC staff has commented that privacy is "a form of nonprice competition important to customers that could be actionable." A transaction that is based largely on the acquisition of personal information may require more time for regulators to evaluate.

An organization seeking to acquire another entity also should carefully evaluate the target's existing privacy and security-related documentation. Key documents include privacy notices distributed by the target entity; information security policies and procedures, including an incident response plan; privacy and information security training and awareness materials; contracts with third-party service providers that have access to personal information; internal and external privacy compliance reviews, assessments or audits; cross-border data transfer documents; and data processing registrations with relevant government authorities.

The due diligence checklist should be customized based on the profile of the target entity. Health care providers and financial institutions are just two examples of types of entities that are heavily regulated by U.S. privacy laws and may require more privacy and data security-related due diligence than, for example, an industrial manufacturer. Depending on the amount and types of personal information the company collects, and how it uses and discloses the information, there may be a large number of

documents to review. Depending on its risk tolerance level, the acquiring company may need to limit the scope of the due diligence. For example, the purchaser might choose to review only critical service provider contracts to understand the privacy and data security provisions they contain. In addition, some deals occur more quickly than others and time constraints may further limit the amount of due diligence that may be performed. Any limitations on due diligence will need to be addressed through other means, however, such as more stringent privacy and data security provisions in the deal documents or an escrow account to address potential post-closing liabilities.

Addressing Privacy and Data Security Issues in Deal Documents

The transaction documents between the parties should contain detailed provisions concerning privacy and data security issues to minimize surprises after the agreement has been signed and the transaction completed. One of the most important provisions is the definition of "personal information" for purposes of the transaction. Although the definition of this term varies depending on the legal regime at issue, it generally should encompass any information that can be linked to an identified or identifiable individual. Depending on the nature of the transaction, an acquiring company that is focused on privacy and data security issues would be wise to insist on a broad definition of personal information and might choose to include specific examples of data elements that meet the definition. The definition of personal information also might need to be customized for transactions that are sector-specific or international in scope.

Acquiring companies should also focus on privacy and data security-related representations and warranties made by the target. These could include, for example, representations that a target entity has complied with applicable privacy and data security laws and industry standards, which range from broad requirements that apply to most companies (such as anti-spam laws) to more narrow requirements (such as the Payment Card Industry Data Security Standard). Companies also should ensure that any disclosure schedules that accompany the deal documents include events that reflect on the privacy and data security practices of the target entity. For example, companies should disclose information security breaches they have experienced during a given look-back period that resulted in notifications to affected individuals or regulators.

Finally, the acquiring entity should require the target to improve its privacy and data security practices during the pre-closing period. For example, these provisions could obligate the target to develop and implement administrative, physical and technical safeguards to protect personal information. These promises also could be more prescriptive, such as requiring that all company-issued devices be encrypted prior to closing the deal. Another covenant could obligate the target to revise pre-closing its public-facing privacy policies, notices or statements as necessary to comply with relevant laws.

Post-Closing Activities

After the transaction has closed, the acquiring party immediately should develop a plan to address privacy and data security issues that require remediation. The plan should prioritize higher-risk data-related issues and seek to resolve those issues as soon as possible post-closing. These could involve consolidating different online privacy policies, aligning access control standards or migrating data centers. All of these decisions could require significant post-acquisition resources and attention.

Following resolution of the high-risk issues, the acquiring entity can move on to address the remaining items. Just as a company may face difficult decisions regarding which key personnel to retain following a merger or acquisition, it also must make critical decisions about how it will use, disclose and protect personal information going forward. These decisions ultimately can determine whether the transaction succeeds or fails in the long run.

Lessons Learned

Companies that make the mistake of acquiring entities whose data retain significant use restrictions or that have inadequate data security practices run the risk of inheriting liabilities for which they did not bargain. In the privacy and data security arena, the buyer must indeed beware.

Lisa J. Sotto is a partner and chair of the global privacy and cybersecurity practice at Hunton & Williams in New York. She assists clients in identifying, evaluating and managing privacy and information security law risks. She may be reached at (212)309-1223 or lsotto@hunton.com. Ryan P. Logan is an associate in the same office. His practice focuses on privacy, data security and records management. He may be reached at (212) 309-1289 or rlogan@hunton.com.