An Expert's View: Key Privacy and Data Security Issues in M&A

PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

Christine Lyon is a partner in the Palo Alto office of Morrison & Foerster LLP. Christine's practice focuses on privacy and employment law. She assists clients in developing global strategies to comply with laws regulating the collection, use, disclosure and transfer of personal information about their customers and employees.

Christine explores issues relating to privacy and data security that often arise in M&A transactions:

What are key considerations for buyers and sellers when negotiating privacy and data security representations and warranties in M&A agreements? How might they approach differ depending on the transaction structure?

Both parties need to understand the nature of the target business, and the privacy issues associated with that business, in order to frame an appropriate set of representations and warranties.

The buyer will want to ensure that the representations and warranties are well tailored to the business and are broad enough to address any applicable privacy risks. For example, a buyer should seek different privacy-related representations and warranties when acquiring a US company that sells hardware to enterprises than when acquiring a multinational, consumer-facing e-commerce business. Even the definition of "personal information" used in the agreement may differ depending on the jurisdictions and laws at issue. In contrast, the seller will want to ensure that the representations and warranties are not overreaching based on the scope of the target business and its operations.

In a merger or stock purchase, the buyer should be concerned about all aspects of the target's privacy and data security compliance because any liabilities are likely to follow the business as a matter of law.

In an asset purchase, by comparison, the buyer will usually focus its privacy-related due diligence on the subset of personal information to be acquired. Even if the buyer is not assuming past liabilities, it should still seek representations and warranties that the seller has complied with applicable laws in collecting this information, including by providing sufficient notice and obtaining any legally-required consent.

Asset purchases also raise additional issues related to the transfer of personal information from the seller to the buyer. A buyer will therefore typically seek representations and warranties that the transfer of this information to the buyer is permissible and will not violate any of the seller's commitments.

Both parties should take special care in addressing disclosures of data security breaches, especially details that are not publicly available. It may not be in the best interests of either party to include overly detailed disclosure schedules. Rather than attempting to allocate risk through a detailed disclosure schedule, the parties may instead consider other ways to allocate the risks from a security breach, such as through special indemnities or holdbacks from the purchase price.

What specific issues and practices relating to privacy and data security matters should both parties consider during the due diligence process?

From the buyer's perspective, it is important to understand its objectives for the transaction and how it intends to use any acquired personal information. In particular, if the buyer seeks to leverage or share this personal information in new ways, it will need to:

- Assess the terms under which that information was collected and any relevant restrictions.
- Evaluate what additional measures may be required to use the information in those new ways. In some cases, this may involve obtaining consent from the seller's or target's customers.

The buyer will want to consider whether any restrictions it identifies affect the value of the deal. If so, the buyer may try to shift some of the risk and obligation to the seller, such as by requiring pre-closing remediation when feasible, or through holdbacks or other economic terms.

From the seller's perspective, it is important to consider applicable privacy laws in assessing what consumer, employee or other personal information may be disclosed during the due diligence process. For example, a seller should avoid disclosing employees' Social Security numbers or other sensitive information, like health information. If the target business has employees outside the US, the seller should remember that many countries limit the disclosure of personal information during the due diligence process, and it should restrict its disclosure of employee data accordingly.

As is often the case, the seller maybe under pressure to disclose large volumes of information quickly during the due diligence process. The seller, however, still needs to exercise care. If it discloses information inappropriately, this may itself raise questions for the buyer about privacy and data security compliance.

What additional concerns might a buyer have when the target business involves cross-border data transfers or must comply with industry-specific data regulations, and how should these be addressed?

When the target business involves cross-border data transfers or industry-specific privacy regulations, the buyer will need to explore the seller's or target's compliance during the due diligence process.

For example, if the seller or target has certified to the EU-US Safe Harbor program, the buyer will want to review any Safe Harbor assessments and other internal compliance materials, as well as its publicly available Safe Harbor certification. If the seller or target is subject to HIPAA, the buyer would want to evaluate its HIPAA compliance measures.

While the buyer may also seek specialized representations and warranties about compliance with these obligations, these contractual measures should not be in lieu of conducting due diligence in these areas. Due diligence is essential.

For the links to the documents referenced in this note, please visit our online version at **www.practicallaw.com/9-544-5025**