Bloomberg Law

Professional Perspective

Navigating Privacy and Data Security Issues in M&A and Other Transactions

Lisa J. Sotto and Ryan P. Logan,
Hunton Andrews Kurth

Navigating Privacy and Data Security Issues in M&A and Other Transactions

Contributed by Lisa J. Sotto and Ryan P. Logan, Hunton Andrews Kurth

Given the value of personal information as a significant corporate asset, companies seeking to acquire or merge with another business should focus carefully on the data they will obtain as a result of the transaction. In addition, as cybersecurity attacks continue unabated, companies must carefully evaluate how personal information maintained by a potential target is protected.

In today's fast-evolving digital environment, deal lawyers must chart a course to navigate privacy and data security issues in corporate transactions. Legal frameworks involving U.S. federal and state law, the European Union's General Data Protection Regulation, antitrust law, and other relevant legal regimes may affect how a company can use personal information following a transaction. This article sets out key questions companies should ask during the due diligence process, discusses how answers to those questions impact the deal documents, and offers post-closing strategies companies should consider.

Legal Considerations

Multiple sources of law constrain the use and disclosure of personal information during and after an acquisition. It is crucial for deal lawyers to contemplate at the outset of a transaction the relevant statutory and regulatory requirements related to personal information. In the U.S. in particular, these requirements often are sector-specific and may dictate the kinds of information that may be disclosed, and how, in the context of a corporate transaction.

U.S. Federal Law

At the federal level, the Federal Trade Commission is the primary federal regulator for data privacy and security in the U.S. The FTC invokes the power granted to it under the FTC Act, which prohibits unfair or deceptive trade practices. To comply, an acquiring entity must either honor the privacy promises the target made to consumers when it initially collected their personal information or, if the entity wants to materially change how it collects, uses, or discloses the data, obtain the individuals' consent before doing so. Awareness of a target's prior privacy representations—the details of which may be drawn out during the due diligence process, discussed below—is important, as a buyer may be bound by them.

Sectoral laws also impact mergers and acquisitions. For example, the Privacy Rule promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 allows a covered entity (such as a hospital, pharmacy, or health plan) to disclose protected health information for its own "health care operations" without obtaining the permission of the individual whose health data is disclosed.

"Health care operations" are defined 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." The path for covered entities is clear, as the transfer of health information between them—for example, in an acquisition of one hospital by another—is free of the regulatory burdens imposed on deals involving non-covered entities.

In another example, the Gramm-Leach-Bliley Act's Privacy Rule allows a financial institution to disclose its clients' nonpublic personal information in connection with a sale, merger, or transfer of all or a portion of the business or an operating unit—but only with respect to the data of clients in the business or operating unit at issue. For any transaction that might implicate U.S. privacy laws, it is critical to identify at the outset which laws apply and which requirements will govern the transfer and future use of the relevant personal information.

U.S. State Law

In the U.S., a combination of the GDPR and a post-2016 "techlash" inspired the California Consumer Privacy Act of 2018, which is a wide-ranging privacy law that shares certain key principles with the GDPR. To add to the state law mélange, a

number of other states are considering various versions of the CCPA. For current state legislative developments concerning consumer privacy, see here.

The CCPA, which has a 2020 compliance deadline, contains an expansive definition of "personal information" that companies must consider when evaluating privacy and data security in a transaction. The CCPA defines personal information to include "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." This encompasses a large swath of information, such as name, postal, and email address, Social Security number, biometric data, internet activity information and geolocation data, as well as "inferences drawn from any of the information identified" in this definition.

Subject to certain exceptions, the CCPA provides consumers with individual rights with respect to their personal information, such as the right to request that a covered business provide the consumer with access to and certain details about the personal information the business has collected about the individual, request that a covered business delete personal information about the consumer that the business has collected from the consumer, and direct a covered business not to sell the consumer's personal information.

The CCPA is enforceable by the California Attorney General and authorizes a civil penalty for violations of the privacy provisions of up to $7,500 per violation. The Act also provides a private right of action in connection with data breaches if a business failed "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." In that case, the consumer may bring an action to recover damages up to $750 per incident or actual damages, whichever is greater.

More generally, the use, disclosure and protection of personal information must comply with myriad state privacy and data security laws. Deal lawyers should ensure that they are familiar with these laws and their various requirements, and should endeavor to foresee their impact on a potential transaction. For example, the California Online Privacy Protection Act of 2003 obligates operators of commercial websites and online services to disclose certain information in their privacy policies, including categories of third parties with whom the operator may share personal information.

The target's privacy policies should reflect these and other relevant requirements. Separately, many state laws contain data security requirements, which typically oblige an entity to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information and the nature and size of the business. The target's data security practices should be scrutinized to ensure that they are, at a minimum, sufficient under applicable law. Of course, acquiring companies also should ensure that they are not inheriting liabilities associated with a prior data breach.

As the examples above illustrate, companies involved in a transaction must have a deep understanding of the personal information the potential target collects and uses, as well as the laws that might apply to such information. Particular attention should be paid to information that intuitively might not be viewed as "personal information." Acquiring entities also should closely evaluate the target's privacy, data security, and individual rights policies and procedures.

European Union

Like the CCPA, the GDPR's definition of personal information is quite expansive. In addition, liability for noncompliance with the GDPR is potentially enormous—up to 4 percent of a company's global annual turnover. Identifying early in a transaction the geographic scope of a deal is imperative, and entails considering matters such as where the target has facilities, whether it offers goods or services to individuals in the EU, whether it monitors EU residents' behavior, and, to the extent the target is obliged to comply with the GDPR, whether it has done so.

Once the acquiring company has moved beyond the threshold question of whether the deal is impacted by the GDPR, it can then move on to analyze specific GDPR-related issues. These include analyzing the legal bases upon which the target processes personal information, determining whether the target has performed data protection impact assessments with respect to high-risk processing activities, determining compliance with cross-border data transfer issues, and reviewing vendor contracts to ensure they comply with the GDPR's requirements for data processors.

Privacy-Related Antitrust Considerations

Antitrust regulators abroad and in the U.S. are increasingly addressing whether, and how, privacy should be viewed in the context of antitrust considerations. In Germany, for example, the Federal Cartel Office, which regulates antitrust issues, recently ruled that Facebook violated German antitrust law by using its market power in the social networking arena to require users to "agree to the practically unrestricted collection and assigning of non-Facebook data to their Facebook user accounts." The president of the FCO admonished Facebook for excluding users who do not consent to the company's data collection practices from Facebook's services and stated that the company "must refrain from collecting and merging data from different sources."

The European Union's competition commissioner, Margrethe Vestager, has publicly focused on the role of data as an antitrust issue. Discussing Amazon, for instance, she said that "the question here is about the data" in announcing a preliminary investigation into Amazon's business practices vis-à-vis its third-party merchants. In contrast, in the U.S., an FTC Commissioner recently stated that antitrust regulators should not attempt to "shoehorn" privacy into antitrust analysis and that there is "little reason to create special antitrust rules" for companies involved in big data analytics.

Despite the differing views of antitrust regulators on the role of privacy in antitrust, companies nevertheless should carefully consider potential antitrust concerns with respect to the transfer and use of personal information in the deal-making process.

Due Diligence, Deal Documents, and Post-Closing Activities

In a corporate transaction, two overarching considerations are key in approaching and assessing the privacy and data security terrain. First, the acquiring party must understand what personal information the target holds and what safeguards are used to protect the security, confidentiality, and integrity of the data. Second, the company should consider how it can use the target's data post-closing.

Assessing the Target's Data in the Context of a Transaction

For an increasing number of companies, data is at the heart of a transaction, and for nearly all businesses, regardless of industry sector, it is essential to pay close attention to the privacy and cybersecurity risks associated with a given target. Accordingly, an acquiring entity's primary task is to conduct due diligence concerning the target entity. One element of such diligence is to ask penetrating questions about the target's privacy and data security practices. Relevant inquiries might include the following:

- In which jurisdictions does the target operate?
- Is the company in material compliance with relevant privacy and data security laws in all the jurisdictions in which it operates?
- What kinds of data processing activities does the target perform?
- Are any such processing activities high risk (e.g., systematic monitoring of the behavior of individuals)?
- Does the target process highly regulated data, such as financial data subject to the Gramm-Leach-Bliley Act? Does the target process sensitive data, such as health or children's data?
- 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?

- Does the company have dedicated employees who are responsible for data privacy and information security?
- Does the company engage in cross-border data transfers?
- Has the company received any complaints or significant 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 in which personal information or other business confidential information has been compromised? Were those events material or systematic?

The due diligence process also involves a review of documents that shed light on the target's information practices. These documents may include information security materials (such as an incident response plan), employee monitoring notices, service provider contracts, internal and external privacy and data security assessment reports, data processing registrations with and other submissions to relevant governmental bodies, and public-facing privacy policies. The process should be crafted in light of the target's particulars; the aim is to discover its data practices—current and past, to the extent relevant—and identify related risks. The results can significantly impact the deal terms, including pricing.

Contract Negotiation

There are standard privacy and data security provisions that appear in most transaction agreements, but they are ideally refined in light of the due diligence process and adjusted as appropriate. For example, the definition of "personal information" should be considered in the context of the particular transaction, including the relevant privacy regimes, and from the buyer's perspective should be expansive (encompassing any information that can be linked to an identifiable individual) so it is sufficiently capacious to capture intended data and widen the scope of the relevant representations and warranties.

Such representations and warranties vary, but at a minimum should address the target's compliance with applicable privacy and data security laws and industry standards, and refer to specific legal regimes, regulators and obligations. They also should cover the target's history of data security incidents and legal proceedings, including enforcement actions. Forward-looking covenants in sale contracts—for example, requiring the target to improve its data security practices in specific ways pre-closing—also are advisable.

Post-Closing Activities

Acquiring entities should develop detailed post-closing strategies that are facilitated through the deal documents. Provisions of this sort may require, for example, creating escrow accounts to address post-closing liabilities, consolidating disparate privacy policies, and improving information security protocols.

Ensuring Smooth Sailing Ahead

Companies that fail to conduct appropriate due diligence into privacy and data security issues during a transaction may face difficulties such as restrictions (or even outright prohibitions) on the use or disclosure of consumer personal information, liabilities associated with data breach class action lawsuits, or shareholder derivative actions. In contrast, companies that conduct thorough due diligence, draft strong and precise contractual protections, and develop comprehensive post-closing strategies may find smooth sailing ahead.

