GIBSON DUNN

Top Data Privacy and Cybersecurity Issues to Think About in M&A Deals

Client Alert | November 14, 2023

An overview of global privacy and cybersecurity considerations and red flags in M&A transactions In today's business environment, data privacy and cybersecurity are bedrocks of trust and confidence—for customers, partners, and other businesses alike. As personal information becomes increasingly digitized, bad actors have augmented cyber-attacks and phishing scams to penetrate business servers and systems. To protect the public, legislators and agencies across the world have passed data privacy and cybersecurity laws to set standards and measures for data privacy and cybersecurity compliance, leading to regulatory, compliance, public relations, and litigation risks. Managing data privacy and cybersecurity risks has become critical to M&A transactions, not only due to the significant exposure to potential legal liability, financial and reputational harm, but also the potential material impact on the company's ability to conduct its operations (especially for data or technology driven companies). The importance of data privacy and cybersecurity is evident from the keen interest of company management in technology, as highlighted by Accenture Research's 2022 Technology in M&A survey, which found that 74% of CEOs view technology integration in M&A as "a source of competitive advantage or growth enabler, rather than the cost of doing business." Furthermore, according to the same survey, 96% of CIOs reported that technology due diligence uncovered "issues or opportunities that had material impact on certain deals." Below, we highlight several privacy and cybersecurity considerations and red flags in M&A transactions, regardless of which side of the table you sit.

1. **Applicability of U.S. State Privacy Laws**

Applicability of the California Consumer Privacy Act, as amended by the California Privacy Rights Act (the "CCPA"), is a critical part of the due diligence process, as the CCPA is enforced by active regulators (both the California Attorney General and the new California Consumer Privacy Agency), and provides a private right of action in the event of certain security incidents. Statutory damages can reach up to $750 per consumer per incident, and CCPA regulatory penalties can be as high as $7,500 per each intentional violation (or $2,500 for unintentional violation). Outside of California, state privacy laws are developing in other jurisdictions as well—13 states have passed laws, with laws in Virginia, Colorado, Utah, and Connecticut taking effect just this year. Closely assessing the applicability of, and compliance with, these various state privacy laws is essential to identifying the legal risks involved for businesses operating and catering to customers in the U.S. As a first step acquirors should review the state-specific threshold requirements for applicability, which may include the target company's gross annual revenue and/or the number of state residents' information processed. For example, the breadth of the CCPA's applicability is particularly broad—any business that has over $25M in revenue a year, and processes personal information of a California resident, will be subject to the law. Notably, any business that says they do not collect personal information—a refrain not uncommon in this area—is likely wrong, if they do business in California or outside the U.S. Indeed, unique amongst the state laws, but more similar to the GDPR, the CCPA applies to information collected from B2B partners, employees, and others not traditionally seen as "consumers," making these laws relevant to nearly every transaction.

2. **Applicability of E.U. / UK GDPR and Other International Laws**

Related People

Ahmed Baladi

Cassandra L. Gaedt-Sheckter

Robert B. Little

Saee Muzumdar

Amanda Estep

Ruby B. Lang

Acquirors should assess whether the target company (i) has any establishment in the E.U. or UK, (ii) even in the absence of an establishment in the E.U. or UK offers goods or services to individuals in the E.U. or UK, or (iii) monitors the behavior of individuals in the E.U. or UK. If the General Data Protection Regulation, including as incorporated into UK law pursuant to the European Union (Withdrawal) Act 2018 (together, the "GDPR"), applies to the company, an acquiror should review the safeguards instituted to ensure safe transfer of personal information outside the European Economic Area ("EEA"). The GDPR also has complex and demanding compliance requirements including, but not limited to, (1) a requirement for controllers to notify supervisory authorities of security incidents within 72 hours, (2) enlistment of processors, by controllers, who contractually agree to implement safeguard required by the GDPR, and (3) stringent restrictions concerning cross-border data transfers to countries outside of the EEA and UK. With increasingly high fines from public enforcement, and growing private enforcement through privacy litigation, the potential consequences of failing to comply with the GDPR are growing. Non-compliance with the GDPR can result in fines up to 20 million Euros, or up to 4% of the total worldwide annual turnover of the company's preceding financial year. Since the GDPR entered into application in May 2018 until October 2023, more than 1,878 fines were imposed amounting to more than EUR 4.4 billion in total. The competent supervisory authorities may also impose other sanctions, such as a temporary or definitive limitation (including a ban) on processing. In addition to civil penalties, there can also be potential criminal liability in some E.U. member states. The legal landscape in the E.U. and UK also continues to evolve, particularly as new laws continue to go into effect in furtherance of the EU Commission's European Data Strategy. The GDPR is also influencing new data privacy laws in other parts of the world, including the Middle-East and APAC regions. Australia, New Zealand, and Singapore have enacted GDPR-like enhancements, and other APAC countries are exhibiting a clear trend towards GDPR-like extra-territoriality and revenue-based fines.

3. **Applicability of Sector-Specific Privacy and Cybersecurity Laws**

Businesses can be regulated by sector-specific or information-specific privacy laws, such as the Health Insurance Portability and Accountability Act ("HIPAA"), the Fair Credit Reporting Act ("FCRA"), the Gramm-Leach-Bliley-Act ("GLBA"), the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), the Children's Online Privacy Protection Act ("COPPA"), the Biometric Information Privacy Act ("BIPA"), the CAN-SPAM Act, and the Telephone Consumer Protection Act ("TCPA"). It is important to assess if any of these sector-specific laws are applicable in light of the nature and activities of the target company. Failure to comply with requirements of such laws can be important red flags, as non-compliance can result in statutory damages, which are assessed on a per-incident basis, including exposing companies to class action suits, under certain laws. While some of these laws are very sector-specific, some (such as CAN-SPAM), may be a reasonable line of inquiry in nearly every transaction.

4. **Outdated Privacy Notices or No Privacy Notice**

Today, it is uncommon to find a brick-and-mortar company with no online presence, and no requirements or best practices to have transparent notices around the collection, processing, transfer, disclosure, sharing, storage, security, and use of personal information. Common red flags for privacy notices include having (1) no policy, (2) an outdated policy, (3) only an online policy (e.g., regarding collection of information online, but not relating to other parts of their business), (4) an online policy that does not match the data collection and processing practices of the target company, or (5) a policy that does not outline consumers' rights related to their personal information.

5. **Storage of Sensitive Personal Information**

A target company may house important and sensitive personal information regarding its employees, customers, suppliers, and counterparties—if not end-consumers. Assessing how such sensitive data is stored, including whether it is stored in-house or through a third-

party vendor, is an important initial step to assess risk. Acquirors should also inquire what security mechanisms are employed by the company, such as whether data at rest and in transit is encrypted using industry-grade mechanisms. If privacy laws are likely to apply, then there may be additional obligations relating to sensitive information (including under U.S. state privacy laws, the GDPR, HIPAA, the GLBA, and others) that should be analyzed.

6. **Cybersecurity Protocols, Policies and Procedures, and Insurance**

Companies are increasingly expected to establish cybersecurity protocols, policies, and procedures, and to conduct security trainings, audits, penetration tests, or other reviews of the company's privacy and cybersecurity protections, and to address any material issues, vulnerabilities, or other risks in a timely manner. The target company's cyber liability insurance policies, and whether any claims have been made against such policies, are also relevant. As acquirors draft representation and indemnification protections concerning cybersecurity matters, it is necessary to review the insurance coverage cap and the categories of attacks covered by the policies.

7. **AI Solutions**

As companies are increasingly relying on AI solutions, acquirors should review whether the target company uses any AI products to assist the business, the type of AI products used, and analyze the scope and types of personal information stored and used by such AI products. Use and/or development of such tools can unveil a gamut of potential risks, including relating to privacy, IP, antitrust, and employment.

8. **Security Incidents, Reports, Investigations, or Litigations**

A crucial aspect of data privacy and cybersecurity diligence is the discovery and disclosure of details regarding past or present security incidents, inquiries, complaints, investigations, or litigation related to personal information. These issues are ubiquitous and important considerations that can affect negotiations for representations and warranties insurance and deal prices. As such, an acquiror should scrutinize, and the target company should disclose:

> Any data privacy or security incidents, which can include (1) the nature of the information affected, including whether any personal information was affected, (2) whether the target company was required to notify individuals or regulators, (3) the extent of any impacts on the target company's operations and revenue, (4) any remediation steps taken to prevent similar incidents from occurring, and (5) whether such incidents have led to any complaints by customers, or inquiries or investigations from relevant governmental authorities. Any risk monitoring mechanisms and practices to prevent these incidents and resultant legal issues. Even if the target company has not experienced any security incidents, an acquiror must review the target company's risk monitoring mechanisms and practices, to ensure the company has measures in place to detect security incidents, and IT and cybersecurity policies and procedures to ensure preparedness, including whether a written information security policy, incident response plan, and business continuity and disaster recovery plan have been developed and implemented. These are all important indicators of a target company's capacity to identify and respond to security incidents and other material system outages or instances of unauthorized access. Acquirors should also be prepared to review data privacy or cybersecurity-related lawsuits or regulatory inquiries, settlements, and claims. These may arise in the context of the target company's session replay litigation, regulatory inquiries in relation to BIPA, CCPA, and the FTC. More specifically, acquirors should be aware of target company's data privacy practices because issues, such as lack of consent from customers, can lead to post-acquisition claims and inquiries concerning the absence of proper compliance measures for processing personal information.

Integrating the Diligence Privacy and cybersecurity diligence can often reveal issues that are not readily apparent to an acquiror, some of which may be material, and some which may not be. Notwithstanding a target company's disclosure of significant breaches and incidents in the disclosure schedule, other material red flags, including insufficient privacy policies or non-compliance with international, domestic, or local privacy and cybersecurity laws, can heavily influence the negotiations involved in draft agreements. Privacy and cybersecurity diligence may influence not only the price associated with the representations and warranties insurance, but also the price of the acquisition or merger itself. If a target company fails to adhere to relevant data privacy laws, post-closing remediation may be necessary to address any existing compliance gaps—for which an acquiror will have an early advantage in constructing adequate compliance measures, if diligence is performed well. Our attorneys are leading industry experts, and we regularly advise on privacy and cybersecurity matters on behalf of the world's largest companies. We efficiently identify the costs and resources needed to implement post-acquisition remediation, and assist in integrating the privacy and cybersecurity practices of target companies into acquirers' global organizations. We also help manage target companies' pre-existing security incidents and claims, and provide holistic assessments on the impacts of such events on the transaction or the acquiror's business.

The following Gibson Dunn lawyers assisted in preparing this alert: Alexander Southwell, Ahmed Baladi, Cassandra Gaedt-Sheckter, Robert Little, Saee Muzumdar, Peter Moon, Amanda Estep, and Ruby Lang.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, any member of the firm's Mergers and Acquisitions, Private Equity, or Privacy, Cybersecurity & Data Innovation practice groups, the authors, or the following practice leaders: **Mergers and Acquisitions:** Robert B. Little – Dallas (+1 214-698-3260, rlittle@gibsondunn.com) Saee Muzumdar – New York (+1 212-351-3966, smuzumdar@gibsondunn.com) **Private Equity:** Richard J. Birns – New York (+1 212-351-4032, rbirns@gibsondunn.com) Wim De Vlieger – London (+44 (0) 20 7071 4279, wdevlieger@gibsondunn.com) Federico Fruhbeck – London (+44 (0) 20 7071 4230, ffruhbeck@gibsondunn.com) Scott Jalowayski – Hong Kong (+852 2214 3727, sjalowayski@gibsondunn.com) Ari Lanin – Los Angeles (+1 310-552-8581, alanin@gibsondunn.com) Michael Piazza – Houston (+1 346-718-6670, mpiazza@gibsondunn.com) John M. Pollack – New York (+1 212-351-3903, jpollack@gibsondunn.com) **Privacy, Cybersecurity & Data Innovation:** Ahmed Baladi – Paris (+33 (0) 1 56 43 1300, abaladi@gibsondunn.com) S. Ashlie Beringer – Palo Alto (+1 650-849-5327, beringer@gibsondunn.com) Jane C. Horvath – Washington, D.C. (+1 202-955-8505, jhorvath@gibsondunn.com) Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com) Our lawyers provide an overview of global data privacy and cybersecurity considerations and red flags in M&A transactions. Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

Mergers and Acquisitions

Private Equity

Privacy, Cybersecurity, and Data Innovation