PAUL HASTINGS

PH PERSPECTIVES

May 2016

Follow @Paul_Hastings

Privacy and Data Security Issues in M&A Transactions – A Checklist

By Behnam Dayanim, Paul M. Schwartz & Mary-Elizabeth M. Hadley

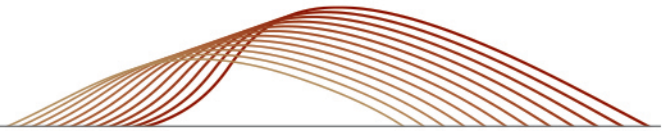
Because the failure of a target company to meet its privacy and data security obligations can present a significant risk to the acquiring company, compliance with applicable laws should be an important consideration in merger and acquisition transactions.

A potential purchaser should seek to understand the nature of the personal information the target collects and the privacy and data security issues relevant to that business. Through due diligence, the purchaser can gain an understanding of the target's rights and obligations regarding the personal information it has collected, retained, used and disclosed.

To assist in that process, this alert provides a checklist of potential privacy and data security issues that may be triggered in mergers and acquisitions.

M&A Privacy & Data Security Checklist

- Existence of Adequate Policies and Procedures
  - Due diligence should include an analysis of the target's privacy policies across all media, including online and mobile. Such policies typically describe the types of information collected, how it is used and with whom it is shared. Importantly, the Federal Trade Commission (FTC) views statements made by companies in such policies as promises—commitments that must be kept even when the company that made them is acquired by another. The failure to keep those promises may lead the FTC to charge the company with violating Section 5 of the FTC Act,[1] which bars unfair and deceptive acts and practices in or affecting commerce and imposes civil penalties of up to $16,000 per violation. State attorneys general may pursue similar actions.
  - The review should also include the target's information security program and procedures, any available external or internal audits conducted and the existence of adequate privacy and data security governance.
- Past Breaches and Security Incidents: A purchaser should request information from the target regarding any history of breaches or security incidents as well as any related notices provided and responses received. Similarly, it is important to identify any past or pending litigation, complaints, administrative fines or penalties relating to privacy and data security issues.



- Direct Marketing Through Text Messaging or Email: Federal laws limit companies' ability to send commercial messages through text messaging or email (as well as other communications media). Understanding a target's activities in this area is essential to an assessment of its potential exposure to regulatory action or litigation.

- Social Media Material: We also recommend requesting information regarding the target's social media presence, activities and policies. Such requests should include, for example, a list of the social media platforms used by the company as well as a description of how the target utilizes those outlets.

- Employment Privacy: A company's email use regulations, social media policies and other aspects of employment privacy can create significant liability issues under employment law.

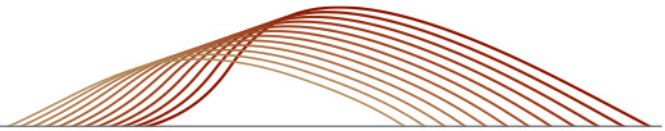
- Sector-Specific Federal Laws: Depending on the target's industry, compliance with a number of federal laws should be assessed, including:

  - **Gramm-Leach-Bliley Act (GLBA):**[2] Requires financial institutions—businesses, regardless of size, that are "significantly engaged" in "financial activities"—to explain their information collection and sharing practices to their customers, tell consumers of their right to "opt-out" if they do not want their information shared with certain nonaffiliated third parties, and safeguard customers' personal information. Notice of breach also may be required. The FTC, along with several other federal agencies and state insurance authorities, is responsible for enforcing the GLBA's requirements.[3]

  - **Health Insurance Portability and Accountability Act (HIPAA)**[4] **and Health Information Technology for Economic and Clinical Health (HITECH) Act:**[5] Require protection and security for the privacy of individuals' health information (PHI). Enforced by the Office of Civil Rights of the U.S. Department of Health and Human Services and state attorneys general, the acts apply to health plans, healthcare providers and healthcare clearinghouses (covered entities) as well as persons who provide certain services to, for or on behalf of covered entities (business associates).[6] The HIPAA Rules also require notice of breaches to federal regulators, patients and, in some instances, media.

  - **Children's Online Privacy Protection Act (COPPA):**[7] Applies to (i) operators of commercial websites and online services (including mobile apps) directed to children under the age of 13 that collect, use or disclose personal information from children, and (ii) operators of general audience websites or online services with actual knowledge that they are collecting, using or disclosing personal information from children under 13. COPPA's primary goal is to place parents in control over what information is collected from their young children online. Operators covered by COPPA must comply with the FTC's regulations regarding the collection, use, disclosure and security of personal information of children under 13.

  - **Fair Credit Reporting Act (FCRA):**[8] Promotes the accuracy, fairness and privacy of information regarding consumers' creditworthiness collected by consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell medical records and rental history records). The FTC, other federal agencies and states



have enforcement authority to seek monetary and injunctive relief against violators of the FCRA's requirements.

- **CAN-SPAM Act:**[9] Issued and administered by the FTC, CAN-SPAM and its implementing regulations impose limitations on the transmission of commercial email messages. Those limitations include the requirement to implement an "unsubscribe" option that enables recipients of the messages to opt out of future commercial emails.

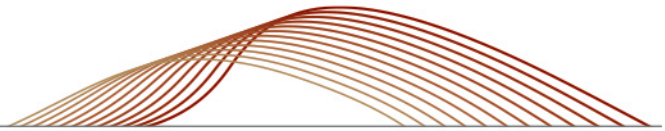
- **Telephone Consumer Protection Act (TCPA):**[10] Imposes restrictions on telemarketing, such as limiting the time of day telemarketers can call residences, requiring that sellers maintain company-specific do-not-call lists and mandating that sellers identify themselves. The TCPA and the Federal Communications Commission's (FCC) rules also limit the use of automatic telephone dialing systems, prerecorded voice messages, faxes and, most significantly, text messages. The statute imposes strict liability for violations and is a fertile ground for class action litigation.

- State Laws: Mergers and acquisitions also may implicate U.S. state privacy laws, such as:

  - **Data Breach Notification Laws:** Forty-seven states, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have enacted laws requiring consumer notification when there is a security breach involving personal information. Notice also may be required to state regulators, media and consumer reporting agencies. Understanding whether a breach has ever taken place at the target company, and whether the required notices have been provided, should form an important focus of diligence.

  - **Security Procedures Laws:** Some states have imposed obligations on persons and entities that own or license their residents' personal information. Most notably, data security regulations in California and Massachusetts require covered organizations to develop, implement and maintain reasonable information security programs. For example, the Massachusetts law requires that an information security program contain appropriate administrative, technical and physical safeguards such as encryption of personal information stored on laptops or other personal devices. The Massachusetts and California laws can apply even if the organization holding the information is not itself located in the Bay or Golden States. Numerous other states require reasonable procedures to be taken when personal information is disposed of or destroyed.

  - **The California Online Privacy Protection Act (CalOPPA):**[11] Enforced by the California Attorney General, CalOPPA requires operators of commercial websites and online services to post their privacy policies conspicuously and specifies what information must be contained in those policies, including the categories of personally identifying information (PII) they collect and the third parties with whom they share that information. The law further mandates that operators disclose (i) how they respond to "do not track" signals or similar mechanisms that provide consumers choices regarding the collection of PII about their online activities over time and across third-party sites and (ii) whether any third parties can collect PII when a consumer uses the operator's website or service.



- **Medical Privacy Laws:** State laws such as California's Confidentiality of Medical Information Act[12]—which prohibits health care providers and recipients of medical information from disclosing patient medical information without authorization unless one of a limited number of exceptions applies—may also be relevant.

- International Considerations: The acquiring company should also assess the target's compliance with privacy and data protection laws in any international jurisdiction where it operates. Certain countries, such as the European Union (E.U.) member states, impose privacy and data security laws that are more far-reaching than U.S. laws. For example, the E.U. Data Protection Directive (E.U. Directive) imposes a detailed set of requirements regarding the collection, use and transfer of personal data. Its recently-approved replacement, the General Data Protection Regulation (GDPR), when it becomes effective in May 2018, will directly bind all E.U. Member States and will impose fines of up to four percent of a company's global revenue for GDPR infractions. In addition, the E.U. imposes restrictions on the transfer of personal data of E.U. residents to countries such as the United States that are not determined to have adequate privacy protections, absent the satisfaction of certain additional requirements. Satisfying those requirements became substantially more complicated following a September 2015 opinion overturning the European Commission's 15-year old decision that the privacy principles of the U.S.-E.U. Safe Harbor provided an adequate level of protection of E.U. citizens' personal data. At least until a new framework is finalized—most likely through the recently-announced Privacy Shield—organizations without alternative mechanisms, such as binding corporate rules (BCRs) or model contracts, may be at risk of violation of E.U. member countries' laws.

By assessing these privacy and data security issues, acquiring companies can manage transactional risk and ensure that the purchase agreement contains provisions that adequately address the target's business and practices. This diligence also should enable an acquirer to step in and effectively manage privacy and data security compliance post-closing.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

New York

James H. Koenig
1.212.318.6005
jimkoenig@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Mary-Elizabeth M. Hadley
1.202.551.1750
maryelizabethhadley@paulhastings.com

[1] 15 U.S.C. § 45.

[2] 15 U.S.C. § 6801 *et seq*.

[3] 15 U.S.C. § 6805. Other federal agencies responsible for enforcing the GLBA against specific financial institutions include the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Board of Directors of the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Board of the National Credit Union Administration and the Securities and Exchange Commission. 15 U.S.C. § 6805(a)(1)-(5).

[4] Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §§ 1320d–1329d-8.

[5] Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 3000 *et seq*.

[6] 45 C.F.R. § 160.103.

[7] 15 U.S.C. § 6501 *et seq*.

[8] 15 U.S.C. § 1681 *et seq*.

[9] 15 U.S.C. §§ 7701 *et seq*.; 16 C.F.R. Part 316.

[10] 47 U.S.C. § 227.

[11] Cal. Bus. & Prof. Code § 22575.

[12] Cal. Civ. Code § 56.