M&A Privacy & Data Security Considerations:

Compliance with Applicable Privacy Laws & Sharing of Customer Information

By:Faith D. Kasparian
January 06, 2015

> Information is everywhere. Indeed, as of 2010, it was noted that "every two days we create as much information as we did from the dawn of civilization up until 2003."[1] And information can be a valuable asset.

Given the ubiquitous and valuable nature of information, the laws associated with information privacy and data security should be a consideration of the due diligence process for a merger or acquisition. In particular, to reduce the risk of potential liability, to prevent roadblocks that may hinder the transaction, and to help ensure that an acquirer can realize the value of the target's customer information, it is important to assess whether the target company: (a) is in compliance with applicable privacy and data security laws; and (b) may share the information of its customers with the acquiring company in connection with (and following) the transaction.

Is the Target Company in Compliance?

Apart from the array of sector-specific privacy and data security laws,[2] there is a varied and rapidly changing landscape of more general state and federal privacy and data security laws that may apply to the target company, depending on the type of information the target collects and maintains.

For example, if the target receives or maintains "personal information"[3] of Massachusetts residents, it has obligations under the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. § 17.00 et seq. These obligations include detailed requirements with respect to maintaining a comprehensive information security program that contains administrative, technical and physical safeguards to protect that information. As another example, if the target operates a website or online service that is directed to children under the age of 13, it has obligations under the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501 et seq. Along the same lines, if the target operates a commercial website or online service and collects even an e-mail address from California residents through the Internet, it has obligations under the California Online Privacy Protection Act, Cal Bus. & Prof. Code § 22575 et seq.

Not only is there an expansive scope of laws that apply to privacy and data security, but the penalties for violations of these laws can be significant. The penalties may require violators to pay substantial monetary fines and to destroy any information or data that was not lawfully obtained.[4] Therefore, to preserve the value of information assets, and (a) as a target, to avoid deterring potential acquirers by concerns of noncompliance liability, and (b) as an acquirer, to avoid assuming the target's noncompliance liability, it is in the best interest of the parties to ensure that the target is in compliance with applicable privacy and data security laws.

May the Target's Customer Information Be Shared with the Acquirer?

Even if a target company is in compliance with applicable privacy and data security laws, the parties also should determine whether the target's customer information may be shared with the acquirer — both in connection with and following the transaction. Aside from any potential liability concerns, making this determination is particularly important from a business standpoint if the information and data concerning the target company's customers is valuable to the acquirer.

Review the Privacy Policy and Ensure That It Is Enforceable

Specifically, the parties should review the target company's privacy policy to understand the circumstances under which the target's customer information may be shared with others. Some privacy policies may include provisions that explicitly permit customer information to be shared in the event of a sale, merger or transfer of all or substantially all of the assets of the respective company. Others may include provisions that explicitly permit customer information to be shared with corporate affiliates (such as entities that control, are controlled by, or are under common control with the company). Or, a policy may specify that information may be shared in these circumstances, but only if customer consent is first obtained.

Not only should the parties review the target company's privacy policy, but to help ensure that the terms of the policy are enforceable, the parties should assess whether the target's customers consented (i.e., through an opt-in or other manifestation of consent) to the terms of the policy. Assuming that the policy is enforceable and addresses the sharing of information with the acquiring company, the parties also must comply with the terms of the policy. Any failure to comply could expose the target to liability under various state and federal laws – including laws prohibiting unfair and deceptive trade practices.[5]

If the Privacy Policy is Silent or Ambiguous, Obtain Customer Consent

If the privacy policy is silent or ambiguous as to whether customer information may be shared with the acquiring company, the recommended course would be to obtain the consent of the target's customers prior to disclosing customer information. While consent could be specific (i.e., consent to disclosure to the particular acquirer) or general (i.e., consent to disclosure to any acquirer), it should be obtained in some manner, as failure to obtain consent could have significant negative repercussions.

As an example, in the analogous context of bankruptcy, an ambiguous privacy policy coupled with failure to obtain customer consent derailed a potential $700,000 sale of information assets. Specifically, in connection with a Chapter 11 bankruptcy proceeding, a bankruptcy trustee sought to sell the assets of *True Beginnings, LLC* ("True"), the operator of the dating website, *True.com*, to the Canadian online dating service, *PlentyofFish.com*. One of the assets at issue was *True.com's* customer database, which included the personal information of *True's* 43 million customers (more than two million of whom were from Texas). Citing consumer privacy concerns, the Texas Attorney General filed an objection to the sale.[6]

The crux of the Texas Attorney General's objection was that *True.com's* privacy policy was ambiguous as to the circumstances under which customer information could be shared. While certain provisions of the policy stated that *True* would not sell or disclose customer information to unaffiliated third parties without the customer's permission, another provision of the policy stated that if *True* should be acquired or substantially all of *True's* assets transferred (and that customers' personal information would be an asset), then customers would be first notified and then given an option to opt-out.[7]

On the basis of the privacy policy's ambiguity, the Texas Attorney General argued that *True's* customers would need to expressly opt-in to the transfer of their information to *PlentyofFish.com*.[8] Shortly after the Texas Attorney General filed its objection, *PlentyofFish.com* withdrew its bid to purchase *True's* assets,[9] and *True* ultimately entered into an Assurance of

Voluntary Compliance agreement with the Texas Attorney General, which, among other requirements, obligated *True* to implement a number of privacy measures.[10]

At the end of the day, the lack of attention to the privacy policy upended the deal. And although this case arose in the context of bankruptcy, the same concerns could apply, and potentially thwart, a merger or acquisition.

Conclusion

As described above, privacy and data security laws are highly relevant to merger and acquisition transactions. To reduce the risk of potential liability, preserve the value of information assets, and decrease the likelihood of privacy and data security-related transaction impediments, it would be prudent to undertake the following steps in connection with the due diligence process:

- Assess the privacy and data security laws that apply to the target and ensure that the target is in compliance with these laws.
- Review and comply with the target's privacy policy, including with respect to the sharing of customer information.
- If the target's privacy policy permits the sharing of customer information with the acquirer, ensure that the target's customers affirmatively consented to the target's privacy policy.
- If the target's policy is silent or ambiguous as to whether customer information may be shared with the acquiring company, obtain the consent of the target's customers prior to disclosing customer information to the acquirer.
- Even if the target's privacy policy permits the sharing of customer information with the acquirer, and the target's customers affirmatively consented to the target's privacy policy, if the customer information at issue is particularly valuable to the acquirer (or is particularly sensitive), consider whether an additional (more timely or specific) consent may be desirable.

If you would like further information on compliance with privacy requirements including in the context of mergers and acquisitions, please contact **Faith D. Kasparian**.

The author would like to acknowledge the contributions to this article by, and give thanks to, the following individuals: Evan Segal, Northeastern University School of Law (NUSL) 2015; and Jonathan Miller, (NUSL) 2015.

Footnotes.

1. *See MG Siegler, Eric Schmidt: Every Two Days We Create as Much Information as We Did up to 2003*, Tech Crunch (Aug. 4, 2010) (quoting Google CEO Eric Schmidt).

2. *See, e.g.*, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d et seq.; and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq.

3. The Standards define "personal information" as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security Number; (b) driver's license or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account." 201 C.M.R. § 17.02.

4. *See, e.g., United States v. Playdom, Inc.*, Case No. SACV 11-0724-AG(ANx), *Consent Decree and Order for Civil Penalties, Injunction and Other Relief* (C.D. Cal. 2011) (available at) (Playdom fined

$3 million by the FTC for violating the Children's Online Privacy Protection Act, 15 U.S.C. § 6501, et seq.); *Resolution Agreement Between U.S. Dept. of Health and Human Services and Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc.* (Sept. 13, 2012) ($1.5 million fine for failure to adequately assess data security risks or adequately adopt or implement security procedures to protect private data); Press Release, *South Shore Hospital to Pay $750,000 to Settle Data Breach Allegations* (May 24, 2012) (available at) (South Shore Hospital agreed to a $750,000 fine for breach of the Massachusetts Consumer Protection Act and HIPAA for failure to adequately put in place procedures to safeguard private data); Press Release, *Major Boston Restaurant Group That Failed to Secure Personal Data to Pay $110,000 Under Settlement with AG Coakley* (March 28, 2011) (Restaurant group paid a $110,000 fine for failing to put in place adequate safeguards to protect customer credit card data and failing to adequately secure its wireless network); see also, *In the Matter of Sears Holding Mgmt. Corp.*, Docket No. C-4264 (Aug. 31, 2009) Decision and Order (Sears ordered to destroy all data collected through tracking software after failing to adequately notify consumers that the software collected data from consumers' secure browsing sessions and third-party website visits); *In the Matter of Upromise, Inc., Docket No. C-4351 (Mar. 7, 2012), Decision and Order* (company ordered to destroy all data collected through a web browser toolbar after failing to adequately notify users of the extent to which it collected information).

5. *See, e.g.* 15 U.S.C. § 45 ("Section 5 of the FTC Act"); M.G.L. c. 93A; 18 PaC.S.A. § 4107(10) (expressly referencing a knowingly false or misleading statement in a privacy policy as a deceptive or fraudulent business practice); see also Federal Trade Commission, *Enforcing Privacy Promises* (stating, "When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. . . . In these cases, the FTC can charge the defendants with violating of Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce" and citing numerous cases arising under Section 5 of the FTC Act for failure to comply with privacy promises).

6. In re: *True Beginnings, LLC*, Case No. 12-42061 (U.S. Bank. Ct., E.D. Tex. 2013), *Texas Attorney General's Objection [To Protect Consumer Privacy] to the Trustee's Motion to Approve Sale* under 11.U.S.C. 363(b)(1)

7. Id. at ¶¶5-6.

8. Id. at ¶¶ 37-53.

9. In re: *True Beginnings, LLC*, Case No. 12-42061 (U.S. Bank. Ct., E.D. Tex. 2013), *Notice of the Termination of the Asset Purchase Agreement Between the Chapter 11 Trustee and Plenty of Fish Media, Inc.*, and Exhibit A thereto (citing the Texas Attorney General's objection and stating that the grounds for the withdrawal of the bid include (among others) that: the sale of True's customer information appears to violate its privacy policy; True does not appear to have the unrestricted right to sell the trade secrets that make up its customer information; there appear to be restrictions on True's right to sell its customer information; and the transfer of True's customer information does not appear to be legal).

10. *In the Matter of State of Texas and True Beginnings d/b/a/ True.com*, Case No. 12-42061 (Tex. Civil Dist. Ct. Travis County 2013), *Assurance of Voluntary Compliance.*