Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Privacy Policies And Asset Sales: It Pays To Plan Ahead

Law360, New York (October 30, 2015, 1:25 PM ET) --



Amy G. Pasacreta Emily S. Tabatabai Shea G. Leitch

Personal data is a valuable corporate asset. At times, the personal information collected from customers (such as email address, mailing address, phone number, etc.) can be a company's most valuable asset. Unfortunately, when a company attempts to sell this asset, it can find the value of the data significantly diminished due to promises made in a privacy policy the company implemented years before it ever contemplated such a sale.

A company's privacy policy sets forth the company's promises to its consumers as to how it will collect, store, maintain and share the consumers' personal data. In an attempt to appeal to customer privacy concerns, it is common for a company to proclaim in such policies:

"We share your personal data only in the ways described in this policy,"

or

"We care about our customers and we will never sell or share your personal data."

Most companies include these statements to highlight their promise not to capitalize on a consumer's data by selling to third-party marketers. However, many companies do not realize that statements such as these could also severely restrict the company's ability to sell data as a corporate asset in a company sale, merger, bankruptcy or similar corporate transaction, unless there is also a clear statement within the policy that permits data to be transferred during the course of such events.

There are steps a company can take leading up to the corporate transaction to smooth the transfer of customer data, such as updating its privacy policy, providing additional notice to consumers, requesting

opt-out or opt-in consent to the revised policy and/or the data sale. Companies that fail to take these steps and attempt to transfer data in a manner that conflicts with promises made in its privacy policy may face regulatory scrutiny or litigation, both of which would ultimately diminish the value of their data assets in any eventual sale.

Enforcement Actions for Violations of Privacy Policies

Most consumers are accustomed to seeing (and, often, ignoring) these privacy policies, which are usually accessed via a hyperlink displayed in small font at the bottom of a Web page. But, while consumers may be ignoring these policies, state and federal regulators — most importantly the Federal Trade Commission and state attorneys general — are not. In fact, these regulators consider a company's privacy policy to be a binding obligation to its customers.

The FTC and state attorneys general can investigate and bring enforcement actions against companies that engage in unfair or deceptive acts and practices,[1] and routinely use this power to investigate whether companies act contrary to the promises made in their privacy policies. Citing breaches of company privacy policies, the FTC has initiated enforcement actions alleging deceptive acts and practices against Google, Snapchat and Myspace, among others. When regulators prevail in their enforcement actions, they may impose a range of penalties upon companies, including injunctions against proposed data use or the deletion of improperly obtained data, customer redress in the event of customer harm, the imposition of a government-written data privacy and security program, record-keeping requirements, and biannual third-party audit and reporting requirements for up to 20 years.

Enforcement Actions Involving Data Sales

The FTC and state AGs keep an eye on companies engaged in high-profile corporate transactions to make sure consumers' privacy rights are not trampled in the companies' haste to consummate deals. The FTC's letter to Facebook and WhatsApp, for example, warned the companies to exercise caution in integrating WhatsApp data into the Facebook family of companies, as WhatsApp's promises to its consumers under its privacy policy were far more restrictive than Facebook's. The FTC further admonished the companies that they must get affirmative consent of WhatsApp users before making any material changes to the WhatsApp privacy policy, lest the companies commit a Section 5 violation.

The Toysmart.com Bankruptcy Precedent

Toysmart.com's Chapter 11 bankruptcy was the first time a federal privacy regulator publicly intervened into a company's bankruptcy. Toysmart was attempting to sell its consumer data, including names, addresses and shopping preferences of consumers as well as family profile information and names of children, to a third-party purchaser as part of the liquidation of its corporate assets. The FTC sued Toysmart for a Section 5 violation in federal court, seeking to enjoin the sale of the data because Toysmart's privacy policy promised that the information it collected would "never be shared with third parties." The parties eventually reached a settlement to permit the sale of the data, but not as a stand-alone asset. The data could be sold as part of the sale of other corporate assets, but only to a "qualified buyer" in a related market that would continue the business as a going concern. Under the settlement, the buyer was required to abide by Toysmart's privacy policy and to obtain opt-in (i.e., affirmative) consent before making material changes to the privacy policy.[2] These restrictions substantially reduced the pool of potential buyers and significantly limited the ways in which the eventual purchaser could use the data. Ultimately, the restrictions proved to be too onerous, and Disney Corp., one of Toysmart's major investors, paid the debtor $50,000 to destroy the data prior to Toysmart's dissolution.

In response to the Toysmart case, Congress enacted Section 363(b)(1) of the Bankruptcy Code. This provision restricts debtors' ability to sell personal information outside the ordinary course of business unless the sale is in compliance with relevant nonbankruptcy law and the sale is either: (1) consistent with the debtor's privacy policy terms, or (2) the court approves the sale after the sale is reviewed and approved by a court-appointed consumer privacy ombudsman. Pursuant to Section 332(b) of the Bankruptcy Code, the consumer privacy ombudsman is appointed "to appear and to be heard at [the sale hearing] and [to] provide the court information to assist the court in the consideration of the facts, circumstances and conditions of the proposed sale or lease of personally identifiable information. ..." The consumer privacy ombudsman is often a bankruptcy practitioner or an attorney from the FTC.

RadioShack's Sale Under Section 363 of the Bankruptcy Code

As RadioShack recently discovered when it attempted to sell its customers' data in Chapter 11, Section 363 of the Bankruptcy Code can pose significant challenges to debtors who fail to exercise foresight when drafting their privacy policies.

Like Toysmart, RadioShack's online privacy policy promised consumers that:

"We will not sell or rent your personally identifiable information to any one at any time,"

and

"Information about you specifically will not be used for any purpose other than to carry out the services you requested from RadioShack and its affiliates. All of our affiliates have agreed to maintain the security and confidentiality of the information we provide to them."

To make matters worse, RadioShack displayed signs in its brick-and-mortar stores declaring:

"We respect your privacy"

and

"We do not sell mailing lists"

Thus, when RadioShack proposed the sale of consumer personal information in bankruptcy, state and federal regulators intervened to block the sale. The FTC warned the court-appointed consumer privacy ombudsman[3] that the proposed sale would violate the FTC Act's prohibition against unfair or deceptive trade practices. The attorneys general of Texas, Oregon and Tennessee also formally objected on the basis that the sale would violate their state consumer protection statutes, and 36 other states joined Texas' objection. Each regulator asserted that RadioShack's proposed sale would violate the explicit terms of its privacy policy, and thus constitute an unfair and deceptive practice in contravention of applicable nonbankruptcy law.

To prevent any such violation, the FTC proposed restrictions on the sale similar to those applied in the Toysmart.com case. After months of collateral litigation, the consumer privacy ombudsman recommended that the sale go forward under limited conditions. The ombudsman recommended that the sale:

- include seven data points, as opposed to the 170 data points originally contemplated;

- not include customers' credit or debit card numbers, Social Security numbers, telephone numbers, or dates of birth;
- only include email addresses from customers active within two years prior to the sale;
- provide an opt-out option to consumers prior to transfer; and
- require the buyer to agree not to sell or share email addresses with any third-party and to abide by RadioShack's privacy policy.

While the sale was ultimately consummated based on the terms set forth above, the majority of the data was destroyed, stripping away much of the data's value to the purchaser.

Quirky's Attempts to Sell Data Assets in Bankruptcy

At the beginning of October 2015, a U.S. bankruptcy trustee objected[4] to bankrupt online marketplace Quirky's motion to sell the data assets belonging to Wink Inc., a Quirky subsidiary that focused on Internet of Things technology that controls basic household systems. While Quirky's privacy policy permits the company to sell user data in connection with a corporate sale or reorganization, that provision of the privacy policy was not added until 2011. The U.S. trustee expressed concern that users who provided data under the pre-2011 privacy policy may not be bound by the revised terms unless they logged in after Quirky changed the policy, and recommended that the bankruptcy court appoint a consumer privacy ombudsman.

Conclusion

These cases highlight the crucial importance of sound privacy policy drafting. Privacy-protective statements that seem innocuous at the drafting stage could — and do — present significant obstacles to the sale of data at the very time the company is under pressure to complete a major corporate transaction. The result could be a loss of significant value for creditors when data assets cannot be sold in bankruptcy, a depreciation of the value of corporate assets to be transferred under a corporate sale, litigation or additional legal costs to sort out data transfer issues, and even the imposition of penalties for a data sale that violates the terms of a company's own privacy policies.

Companies must think about their long-term data needs, and should consider all possible contingencies, such as a future asset sale, restructuring, bankruptcy, and other corporate transactions. Any company considering a corporate transaction or facing financial difficulties should review its existing privacy disclosures and act quickly to modify privacy statements, and if needed, to provide notice and seek consent for such policy changes well in advance of the date of the corporate event or bankruptcy filing. Swift, intelligent action may help companies to preserve the value of their data assets.

—By Amy G. Pasacreta, Matthew Fechik, Emily S. Tabatabai and Shea G. Leitch, Orrick Herrington & Sutcliffe LLP

Amy Pasacreta is a senior associate in Orrick's New York office. Matthew Fechik is an associate in Orrick's Wheeling, West Virginia, office. Emily Tabatabai is a privacy attorney and Shea Leitch is an associate in the firm's Washington, D.C., office.

[1] The FTC exercises broad jurisdiction to bring enforcement actions against companies that engage in unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act. 15 U.S.C. § 45(a). Many states have similar consumer protection legislation, commonly known as the "Baby FTC Acts."

[2] In re Toysmart LLC, Consent Decree, Ex. A, Stipulation & Order Establishing Conditions on Sale of Customer Information, Case No. 00-13995-CJK (July 21, 2000). https://www.ftc.gov/sites/default/files/documents/cases/toysmarttbankruptcy.1.htm

[3] In RadioShack, the court-appointed consumer privacy ombudsman was Jessica L. Rich, the director of the FTC's Bureau of Consumer Protection.

[4] See Objection, In re: Quirky Inc., No. 15-12596 (MG) (Bankr. S.D.N.Y. 2015).