

GC New York

From the publishers of the New York Law Journal

Emerging Privacy Issues in Bankruptcy

By Lisa J. Sotto, Scott H. Bernstein and Boris Segalis
June 10, 2010

The emergence of information privacy issues over the last decade has led to increased scrutiny of public representations that companies make regarding their information practices. As a result of consumer privacy expectations and legal requirements, these representations are typically found in a company's Web site privacy notice. Too often, however, companies make commitments regarding their information practices that are difficult to meet and fail to anticipate changes in business circumstances (such as mergers or sales of assets). Such commitments may prove damaging to the company, its investors and creditors.

When a company makes public representations imposing excessive limitations on its use and disclosure of personal information, it has the potential to significantly diminish the value of the company's personal information assets. One particularly troublesome representation is the inclusion in a privacy notice of a broad assertion that the company "never shares personal information with third parties." If such a representation is untrue, a company risks an enforcement action by the Federal Trade Commission (FTC) for engaging in a deceptive trade practice.¹ If, on the other hand, the representation of not sharing personal information with third parties is accurate, it should raise red flags for the company's investors and creditors, especially when personal information is a significant asset for the company.

One of the little-known circumstances where such excessive representations in a privacy notice can have a significant impact is in bankruptcy proceedings. A broad assertion in a privacy notice, for example, could limit or preclude a bankruptcy sale of assets such as customer lists.

The protection of consumer privacy was one of the issues addressed by the Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA), enacted in 2005, which amended the U.S. Bankruptcy Code.² The BAPCPA amendments imposed certain restrictions on the sale or lease to parties not affiliated with the debtor of personal information that the debtor obtained pursuant to a privacy notice.³ The Code's relevant definition of personal information is broad and includes details such as an individual's name, postal and e-mail address, telephone number, Social Security number and payment card number that an individual provides to a debtor "in connection with obtaining a product or service from the debtor primarily for personal, family, or household purposes."⁴

A debtor whose relevant privacy notice anticipates asset sales involving personal information benefits from the Code's authorization of sales and leases of the information that are consistent with the debtor's applicable privacy notice.⁵ If, on the other hand, the relevant privacy notice is deemed to prohibit transfers of personal information to parties not affiliated with the debtor, the Code requires the appointment of an independent consumer privacy ombudsman to oversee the sale or lease of the information.⁶

The ombudsman's role is to provide recommendations to the bankruptcy court to assist the court in its consideration of the proposed sale or lease of personal information. In providing recommendations to the court, the ombudsman may consider (i) the debtor's relevant privacy notices, (ii) the potential losses or gains of privacy to consumers if the court approves the sale or lease of personal information, (iii) the potential costs or benefits to consumers if the court approves the sale or lease, and (iv) alternatives that would mitigate potential privacy losses or costs to consumers.⁷ The Code requires the court to conduct a hearing and approve the sale only after (i) giving due consideration to the facts, circumstances and conditions of the sale or lease, and (ii) finding no showing that the sale or lease would violate applicable non-bankruptcy law.⁸

Prior to the enactment of the BAPCPA, bankruptcy courts did not view as a significant issue the protection of consumer privacy in connection with asset sales that involved personal information. In 2000, however, the FTC sought to raise the public's awareness of privacy implications of bankruptcy asset sales in the case of *In re Toysmart.com, LLC*.⁹ Toysmart.com LLC sought the bankruptcy court's approval to sell certain assets, including the company's customer lists, through a public auction. Toysmart's applicable privacy notice stated, however, that the company's customers could "rest assured" that their information would "never be shared with a third party." Upon learning of the proposed sale of customer lists, the FTC filed an action in federal court seeking to enjoin the sale.¹⁰

The FTC alleged that the sale was inconsistent with the promises Toysmart made in its privacy notice and, therefore, a deceptive trade practice that violated §5 of the FTC Act. While Toysmart subsequently reached a settlement with the FTC to allow the sale, the attorneys general of 47 states objected to the settlement, which had not yet been approved by the bankruptcy court. Faced with such opposition, Toysmart withdrew the customer lists from the auction and eventually destroyed the information. To prevent similar sales of personal information in bankruptcy, Congress enacted the BAPCPA consumer privacy amendments. Senator Patrick Leahy of Vermont, one of the sponsors of the legislation, stated that the amendments were enacted to "prevent future cases like *Toysmart.com*."¹¹

Consumer Privacy Ombudsman

Following the enactment of the BAPCPA, the appointment of a consumer privacy ombudsman has become standard practice in bankruptcy cases in which personal information, such as customer or Web site visitor lists, is the subject of an asset sale. One of the first applications of the BAPCPA consumer privacy amendments occurred in the *In re Engaging and Empowering Citizenship Inc.* bankruptcy case.¹² In *Engaging*, the debtor was in the business of developing and implementing Internet technology. Specifically, the debtor owned and operated three Internet portals: Earth911.com, Pets911.com and AmberAlert.com. Individuals accessing the Web site portals subscribed to various services by providing personal information, including name, telephone number and e-mail address. The Web site privacy notices pursuant to which the debtor collected the information asserted that the company would not sell, trade or provide any personal information to third parties.

In the course of the bankruptcy proceedings, the court-appointed examiner sought to sell certain of the debtor's assets that included the Internet portals and the corresponding personal information the debtor collected through the portals. The bankruptcy court found that the proposed sale would be inconsistent with the statements in the relevant privacy notices

asserting that the personal information would not be disclosed to third parties. Accordingly, the court ordered the appointment of a consumer privacy ombudsman.

The ombudsman recommended that the court approve the sale, but that the court require the purchaser to (i) adopt the debtor's existing privacy policies, (ii) post on the purchased Web sites a statement permitting individuals who had previously provided personal information through the Web sites to request the deletion of their information, and (iii) upgrade its data security safeguards. Subsequently, the court approved the sale of the debtor's assets, including personal information, subject to the parties' compliance with the ombudsman's recommendations.

Similarly, in *In re Chrysler LLC*, the debtor, Chrysler LLC, sought the bankruptcy court's authorization to sell substantially all of its assets to a Fiat S.p.A. affiliate.¹³ The proposed sale included personal information, such as consumers' names, mailing addresses, e-mail addresses, telephone numbers and financial information collected on Chrysler Web sites and through Chrysler's independent dealers. The privacy notice pursuant to which Chrysler collected the information asserted that Chrysler would not distribute the information to anyone other than affiliated entities. In light of the assertions in the debtor's notice, the bankruptcy court appointed a consumer privacy ombudsman to review and provide recommendations on the proposed sale of personal information.

Similar to the ombudsman's findings in *Engaging*, the ombudsman in *Chrysler* recommended that the court approve the sale subject to significant restrictions. Specifically, the ombudsman recommended that the court require (i) the information to be sold to a purchaser operating in a similar business, (ii) the purchaser to agree to abide by the debtor's privacy notice, (iii) the debtor and the purchaser to provide notice of the proposed sale to consumers whose personal information was subject to the sale, and (iv) the debtor and the purchaser to provide consumers with an opportunity to opt out of the transfer of the information to the purchaser. The ombudsman also recommended the destruction of consumers' financial information, such as Social Security and bank account numbers, in the absence of a compelling business or legal justification for transferring such information to the purchaser.

By contrast, when a proposed bankruptcy sale or lease of personal information is consistent with the debtor's privacy notice, a bankruptcy court is likely to allow the sale without appointing a consumer privacy ombudsman. For example, in *In re Boscov's Inc.*, the debtor, Boscov's Inc., owned and operated a full service department store chain.¹⁴ Boscov's collected personal information on the company's Web site and by other means in connection with order forms, customer service inquiries, credit card applications and other submissions.

In bankruptcy, Boscov's sought to sell substantially all of its assets, including the personal information of its customers. The relevant privacy notice provided that "[i]n the event that some or all of the business assets of Boscov's are sold or transferred, [Boscov's] may transfer the corresponding information about our customers." In light of the language contained in Boscov's privacy notice, the bankruptcy court approved the sale without appointing a consumer privacy ombudsman or imposing other restrictions on the personal information.

Drafting Privacy Notices

Consumer privacy ombudsman decisions in *Engaging* and *Chrysler* and the bankruptcy court's decision in *Boscov's* are a testament to the value of a comprehensive and well-conceived privacy notice. Because the relevant privacy notices in *Engaging* and *Chrysler* did not account for changes in the debtors' business circumstances, the ombudsmen recommended significant restrictions on the sales of personal information, which likely diminished the value of the assets. In both cases, the ombudsmen limited the purposes for which the purchasers could use or disclose the information by binding the purchasers to the debtors' relevant privacy notices. This restriction is especially onerous because, if a purchaser subsequently seeks to revise the privacy notice to change the manner in which the information is used or disclosed, the purchaser may be subject to the FTC's requirement to obtain the affirmative, opt-in consent of the relevant consumers to the proposed changes.¹⁵ In addition, the ombudsmen's requirements that consumers have the opportunity to opt-out of the transfer or have their information deleted reduced the amount of personal information available for the asset sale and, accordingly, likely diminished the value of the information in the sale.

The Bankruptcy Code, as applied in *Engaging*, *Chrysler* and *Boscov's*, establishes a direct link between the quality of the privacy notice and the value of personal information collected pursuant to the notice. A strategic approach to maintaining the value of personal information assets and mitigating against the restrictions ombudsmen and bankruptcy courts may impose on sales or leases of personal information assets requires companies to implement comprehensive and robust privacy notices that anticipate changes in their business circumstances.

A Web site privacy notice should, at a minimum, set forth (i) the types of personal information a company collects on its Web site, (ii) how the information is used, (iii) to whom it is disclosed, (iv) how the company protects personal information, (v) contact information for questions or comments about the company's information practices, and (vi) the notice's effective date. In providing this information, companies should consider their existing privacy practices and anticipate changes in their business.

With respect to uses of the information, a privacy notice should provide the broadest disclosure in light of the company's current and future business needs. For example, a robust notice may disclose various marketing and data analytics purposes for which a company, its affiliates and other third parties may use the information. In addressing disclosures of personal information, a well-drafted privacy notice should inform consumers that, for example, the company may disclose their personal information to service providers, joint marketing partners and other third parties that may offer products or services to the company's customers.

To help address consumer privacy concerns raised by the BAPCPA amendments, the notice also should state that the company may transfer personal information to non-affiliated third parties in the event of a sale or transfer of all or a portion of the company's assets. While companies may commit to use reasonable efforts to direct the purchaser to use the personal information in a manner consistent with this company's relevant privacy notices, consumers should be informed that following the sale or transfer of the information, the purchaser's privacy notices will govern the handling of the information and any concerns about the handling of the information should be directed to the purchaser.

It is important to note that companies in the United States generally have some leeway in choosing how they use and disclose personal information. Legal requirements that mandate privacy notices generally do not impose substantive limitations on the use or disclosure of the information but, instead, require companies to post notices that are accurate and contain certain substantive elements.¹⁶ In addition, with certain exceptions, the FTC has authority pursuant to Section 5 of the FTC Act to investigate and bring enforcement actions regarding misrepresentations in companies' privacy notices, and has brought numerous actions pursuant to this authority.¹⁷ The FTC's enforcement authority extends to privacy notices companies issue both voluntarily and pursuant to legal requirements, but Section 5 does not impose affirmative restrictions on the use or disclosure of personal information.

In light of the consumer privacy protection amendments to the Bankruptcy Code and other legal requirements that may apply to privacy notices, companies should focus considerable efforts on drafting privacy notices that are accurate and robust. While it is critical to address consumers' privacy expectations in preparing privacy notices, it is also important for companies to avoid excessive privacy commitments that may adversely affect strategic business interests now and in the future, including the value of the company's personal information assets.

Lisa J. Sotto is a partner and head of the privacy and information management practice at Hunton & Williams in the New York office, and can be reached at lsotto@hunton.com.

Scott H. Bernstein and **Boris Segalis** are associates at the firm. **Robert A. Rich**, an associate at the firm, and **Aaron P. Simpson**, a partner, assisted in the preparation of this article.

Endnotes:

1. See §5 of the Federal Trade Commission Act ("FTC Act"), 15 USC §45.
2. 11 USC §§101-1532.
3. See 11 USC §363(b)(1).
4. See 11 USC §101(41A). The Code refers to personal information as "personally identifiable information."
5. See 11 USC 363(b)(1)(A).
6. See 11 USC 363(b)(1)(B).
7. See 11 USC §332(b).
8. See 11 USC §363(b)(1).
9. *In re Toysmart.com, LLC*, Case No. 00-13995-CJK (Bankr. D. Mass. June 9, 2000).
10. *FTC v. Toysmart.com, LLC*, Case No. 00-11341-RGS (D. Mass. July 10, 2000).
11. See 151 Cong. Rec. S1781 (daily ed. Feb. 28, 2005).
12. *In re Engaging and Empowering Citizenship Inc.*, Case No. 05-28175 (CGC) (Bankr. D. Ariz. Dec. 15, 2005).
13. *In re Chrysler LLC, et al.*, Case No. 09-50002 (AJG) (Bankr. SDNY April 30, 2009).
14. *In re Boscov's Inc., et al.*, Case No. 08-11637 (KG) (Bankr. D. Del. Aug. 4, 2008).
15. See FTC, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (Feb. 12, 2009), available at <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.
16. Certain sector-specific laws in the United States may both require the posting of a privacy notice and impose substantive restrictions on the sharing of certain personal information. For example, the federal Gramm-Leach-

Bliley Act requires financial institutions to provide a privacy notice to their customers and limits the disclosure of certain personal information. See 15 USC §§6801-6809.

17. See, e.g., *In re Premier Capital Lending Inc.*, No. C-4241 (FTC Dec. 10, 2008) (The FTC alleged that Premier violated §5 of the FTC Act by failing to meet the terms of its own privacy policy).

Reprinted with permission from the June 10, 2010 issue of *GC New York* © Copyright 2010. ALM Media Properties, LLC. All rights reserved.