BAKER DONELSON

CONSUMER DATA PRIVACY IN BANKRUPTCY

John A. Drennan
Of Counsel
Washington, D.C.
202.508.3462
jdrennan@bakerdonelson.com

Bankruptcy law and privacy law may appear to be wholly separate areas of the law, but they overlap more than one might anticipate. Balancing individual rights and interests to achieve a social good is at the heart of both fields. In the privacy arena, privacy interests are pitted against other key social goals, such as national security, research and innovation. Bankruptcy involves similar trade-offs between interests and equities: for example, should creditors be compelled to take a haircut in order to preserve a viable but insolvent going concern or to avoid loss of jobs and harm to communities? Contract rights of all kinds may be altered in bankruptcy to achieve bankruptcy goals; a debtor can cure a breach and pay a fraction of the damages that it inflicted on others, so that the debtor might reorganize and continue. The underlying bankruptcy principle is that if someone can be made better off while leaving everyone else no worse off economically, then this result is socially desirable.

The overlap exists at more than the theoretical level. In the 2005 amendments to the Bankruptcy Code (BAPCPA), Congress passed legislation to protect consumers against the sale of personal identifiable information (PII) by the debtor when the sale would violate that debtor's privacy policy outside of bankruptcy (e.g., if the privacy policy says that such information would not be shared with any unaffiliated third party). The 2005 amendments could have been written to flatly prohibit any such sale, thereby enforcing the privacy rights of the consumers outside of bankruptcy. Instead, they left open the door to transfers of PII that could not occur outside of bankruptcy. Congress thus gave the underlying principle of bankruptcy – making some people better off without impairing anyone else – room to run.

Many companies anticipate and provide for data transfers when their assets are sold in or outside of bankruptcy. Even if a privacy policy does not permit such transfer, the Code provides a special way out: a consumer privacy ombudsman is appointed and the court can approve the sale of PII, contrary to the terms of privacy policy, if it has given "due consideration to the facts, circumstances, and conditions of such sale or such lease" and has found "no showing...that such sale or such lease would violate applicable nonbankruptcy law."

With the participation of the FTC and state consumer-protection authorities, the common approach to PII assets is to protect the underlying privacy concerns of consumers by requiring that the buyer:

(1) is in materially the same line of business as the seller;
(2) is bound by the other terms of the privacy policy; and
(3) provides the consumers with an opt-out right in lieu of their right to consent outside of bankruptcy.

This paper sets forth the relevant law regarding bankruptcy and PII, short descriptions of key cases that have shaped the field and some takeaway lessons to consider when dealing with PII as a company asset.

The U.S. Bankruptcy Code

The amendments to the Bankruptcy Code of 2005 provide a statutory framework governing the transfer, sale or lease of PII in the possession of the debtor. The Code defines PII broadly to include names, residential addresses, email addresses, telephone numbers, social security numbers, credit card numbers and, when "in connection with 1 or more" of these, a date of birth or "other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically":

(A) if provided by an individual to the debtor in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes – (i) the first name (or initial) and last name of such individual, whether given at birth or time of adoption, or resulting from a lawful change of name; (ii) the geographical address of a physical place of residence of such individual; (iii) an electronic address (including an e-mail address) of such individual; (iv) a telephone

number dedicated to contacting such individual at such physical place of residence; (v) a social security account number issued to such individual; or (vi) the account number of a credit card issued to such individual; or

(B) if identified in connection with 1 or more of the items of information specified in subparagraph (A) – (i) a birth date, the number of a certificate of birth or adoption, or a place of birth; or (ii) any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically[.]

BAPCPA § 41A.

Section 363(b)(1) of the Code sets forth the substantive restrictions on the disposition of PII, generally prohibiting the sale or lease of PII when transfer is prohibited by a debtor's privacy policy unless (a) "such sale or lease is consistent with such policy," or (b) after the appointment of a consumer privacy ombudsman," the sale or lease is approved by the court. More specifically, section 363(b)(1) provides:

The trustee, after notice and a hearing, may use, sell, or lease, other than in the ordinary course of business, property of the estate, except that if the debtor in connection with offering a product or a service discloses to an individual a policy prohibiting the transfer of personally identifiable information about individuals to persons that are not affiliated with the debtor and if such policy is in effect on the date of the commencement of the case, then the trustee may not sell or lease personally identifiable information to any person unless –

(A) such sale or such lease is consistent with such policy;

or

(B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease – (i) giving due consideration to the facts, circumstances, and conditions of such sale or such lease; and (ii) finding that no showing was made that such sale or such lease would violate applicable nonbankruptcy law.

11 U.S.C. § 363(b)(1).

Finally, the appointment process for, and duties of, the consumer privacy ombudsman are set forth in Section 332:

(a) If a hearing is required under section 363(b)(1)(B), the court shall order the United States trustee to appoint, not later than 7 days before the commencement of the hearing, 1 disinterested person (other than the United States trustee) to serve as the consumer privacy ombudsman in the case and shall require that notice of such hearing be timely given to such ombudsman.

(b) The consumer privacy ombudsman may appear and be heard at such hearing and shall provide to the court information to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale or lease of personally identifiable information under section 363(b)(1)(B). Such information may include presentation of –

(1) the debtor's privacy policy;

(2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court;

(3) the potential costs or benefits to consumers if such sale or such lease is approved by the court; and

(4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers.

(c) A consumer privacy ombudsman shall not disclose any personally identifiable information obtained by the ombudsman under this title.

11 U.S.C. § 332(a) and (b)(1)-(4).

It has been reported that the consumer privacy ombudsman is most often a bankruptcy practitioner or an attorney from the FTC.

Key Cases

Toysmart.com

Toysmart's Chapter 11 bankruptcy was the first time a federal privacy regulator formally intervened in a company's bankruptcy, and reportedly gave rise to the PII provisions in the Bankruptcy Code of 2005. In 2000, Toysmart attempted 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. The buyer was also 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.

As one would expect, these settlement restrictions substantially reduced the pool of potential buyers and significantly limited the ways in which the eventual purchaser could use the data. Indeed, the restrictions proved so onerous that Disney Corp., one of Toysmart's major investors, ultimately paid the debtor $50,000 to destroy the data prior to Toysmart's dissolution.

Borders Bookstore

In 2011, the FTC sent a letter advocating the protection of personal customer information held by Borders Group, which was in bankruptcy. The letter was addressed to the consumer privacy ombudsman appointed by the court overseeing the Borders bankruptcy. It noted that Borders collected substantial amounts of data from customers, including records of books and videos purchased, and that Borders had promised its customers that it would not share the information without consent.

Borders collected this information under three different privacy policies, each of which represented that customer information would not be rented or sold to third parties except in limited circumstances and then only with the express consent of its customers. The first and second Borders privacy policies, published in 2006 and 2007, respectively, stated in relevant part:

> Borders, Inc., Walden Book Company, Inc., and their related companies believe that your personal information – including your purchase history, phone number(s), and credit card data – belongs to you. We collect this type of information to serve you better when you provide it to us, but we do not rent or sell your information to third parties. From time to time, we may ask if you are interested in receiving information from third parties whose services or information we think would be of value to you. In those instances, we will only disclose your email address or other personal information to third parties if you expressly consent to such disclosure.

The third policy, published in 2008, contained the same language above restricting the sale or rental of personal information, but also described circumstances under which Borders might disclose personal information:

> Circumstances may arise where for strategic or other business reasons, Borders decides to sell, buy, merge or otherwise reorganize its own or other businesses. Such a transaction may involve the disclosure of personal or other information to prospective or actual purchasers, or receiving it from sellers. It is Borders' practice to seek appropriate protection for information in these types of transactions. In the event that Borders or all of its assets are acquired in such a transaction, customer information would be one of the transferred assets. (Emphasis added.)

Despite the fact that the 2008 policy indicated a transfer of customer information would occur if Borders decided to sell, buy, merge or otherwise reorganize its businesses, the FTC downplayed the significance of this language, stating that "[w]e view this provision as applying to business transactions that would allow Borders to continue operating as a going concern and not to the dissolution of the company and piecemeal sale of assets in bankruptcy." The FTC thus recommended to the court that any transfer of personal information in connection with a bankruptcy sale take place only with consent of Borders' customers or with significant restrictions on the transfer and use of the information.

CONTINUED

Ultimately, the bankruptcy court approved the sale of customer information from Borders to Barnes & Noble. The court, however, required that former Borders customers receive an email notification and that the companies place prominent notices on their websites and run advertisements in the newspaper USA Today. The court also required that customers were given 15 days to opt-out of the transfer.

RadioShack

As RadioShack discovered in 2015 when it attempted to sell its customers' data in bankruptcy, Section 363 can pose significant challenges to debtors who fail to exercise foresight when drafting their privacy policies.

Similar to 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."

Additionally, RadioShack displayed signs in its brick-and-mortar stores declaring "We respect your privacy" and "We do not sell mailing lists."

The FTC and multiple State Attorneys General intervened to block the sale of consumer personal information. The FTC warned the court-appointed consumer privacy ombudsman 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's 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 non-bankruptcy law.

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

- 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.

Notably, while the sale was ultimately consummated based on the terms suggested by the ombudsman, most of the data was first destroyed, stripping away much of the value to the purchaser.

Crumbs Bake Shop

In 2014, Crumbs, a publicly-held company selling cupcakes and other baked goods, filed for Chapter 11 protection. The company then filed a motion seeking permission from the U.S. Bankruptcy Court in New Jersey for an auction sale that would include Crumbs' intellectual property, consisting of customer data such as names, phone numbers and addresses.

The U.S. Trustee moved to appoint a consumer privacy ombudsman. The U.S. Trustee argued that auctioning the customer lists would violate Crumb's privacy policy, which provided:

> Crumbs Bake Shop is highly sensitive to the privacy interests of consumers and believes that the protection of those interests is one of its most significant responsibilities. In acknowledgement of its obligations, Crumbs Bake Shop has adopted the following Privacy Policy applicable to information about consumers that it acquires in the course of its business.

> Disclosure to Third Parties. We will provide individually-identifiable information about consumers to third parties only if we are compelled to do so by order of a duly-empowered governmental authority, we have the express permission of the consumer, or it is necessary to process transactions or provide our services.

The U.S. Trustee observed that Crumbs' privacy policy contained three exceptions that would allow sharing of customer information: (1) "we are compelled to do so by order of a duly-empowered governmental authority," (2) "we have the express permission of the consumer," or (3) "it is necessary to process transactions or provide our services." The Trustee reasoned that because "the sale of the customer lists to a third party does not fall within one of the carved-out exceptions, the sale of the lists is prohibited." "To read the policy differently would render the debtors' privacy policy meaningless, leading consumers to believe their personal information is protected when in fact, it is not."

The U.S. Trustee further argued that an ombudsman would assist the Bankruptcy Court in resolving the matter by providing information at a hearing regarding the potential losses or gains of privacy and possible costs or benefits to consumers of the proposed sale, as well as alternatives that could mitigate privacy losses or costs to consumers. The court granted the motion.

Takeaways

The foregoing cases suggest a number of pointers for bankruptcy, M&A and privacy attorneys alike.

First¸ the level of privacy protection provided by a company's privacy policy is inversely proportional to the value of its private consumer data in bankruptcy. Strong restrictions in a privacy policy on sharing private customer data, for example, will likely limit the pool of potential purchasers of a company's customer list, effectively reducing the value of what at first might appear to be a highly valuable company asset. Indeed, as in the Toysmart and RadioShack bankruptcies, such restrictions could even change a potential asset into a liability, because the purchaser will need to pay to have the data destroyed.

Second, while consumers may routinely treat privacy policies as a check-the-box exercise, the story is far different in bankruptcy court. The FTC, state AGs and bankruptcy trustees keep a watchful eye on companies engaged in high-profile corporate transactions to ensure consumers' privacy rights are not trampled in the parties' haste to consummate deals. They are prepared to move the court on behalf of customers to uphold consumer privacy rights. Given the robust enforcement, companies must be aware from the start that there is a trade-off between the privacy assurances they provide to their customers and the value of their customer lists in the bankruptcy and M&A contexts. Where the balance is best struck may be a business issue, but that a balance is struck (even if only inadvertently) is legal fact.

Finally, the language used by consumer-facing companies to craft companies' privacy policies must be exceptionally strong and clear. It is not sufficient to indicate that a company's customer list may be shared if the company sells, buys, merges or otherwise reorganizes its businesses. As we saw in the Borders bankruptcy, just such language was understood by the FTC to apply to business transactions that allow the company to continue operating as a going concern, and not to the dissolution of the company and sale of its assets in bankruptcy. In short, if the client wants a different result, that must be spelled out.

---

i https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding

ii https://www.ftc.gov/es/node/613761

iii https://www.ftc.gov/system/files/documents/public_statements/643291/150518radioshackletter.pdf

iv https://consumermediallc.files.wordpress.com/2015/05/042015229126.pdf

v See https://www.manatt.com/uploadedFiles/Content/4_News_and_Events/Newsletters/AdvertisingLaw@manatt/In%20re%20Crumbs%20motion.pdf