AMERICAN BANKRUPTCY INSTITUTE
JOURNAL
The Essential Resource for Today's Busy Insolvency Professional

News at 11

By Carl Wedoff and David P. Saunders

Big Data Meets Bankruptcy

Will the Increased Value of Consumer Data Lead to a Weakening of Privacy Protections in Bankruptcy Sales?

Carl Wedoff
Jenner & Block LLP
New York

David P. Saunders
Jenner & Block LLP
Chicago

Carl Wedoff is a restructuring and bankruptcy associate with Jenner & Block LLP in New York. David Saunders (CIPP/US) is a partner and member of the firm's Data Privacy and Cybersecurity Practice and Complex Commercial Litigation Practice in Chicago.

Companies have collected consumer data as long as there have been companies, and had merchants note customer preferences to determine what they would sell. In the 1980s, companies used customer transactions for direct-mail marketing, and with the advent of the information age in the 1990s, online companies began collecting more extensive personal information for internet advertising and marketing purposes.[1] In recent years, however, the volume and value of consumer data collection has increased exponentially. The transfer of consumer data has become a major multibillion-dollar industry of its own: In 2018, U.S. companies spent nearly $20 billion acquiring and analyzing consumer data.[2] At the same time, consumer-privacy laws are on the rise at the state level and are under consideration at the federal level.[3] Put lightly, the value of data can result in substantial friction with maintaining and complying with important consumer-privacy interests.

Bankruptcy courts routinely deal with the sale of consumer data, often in retail bankruptcies, but to date "big data" issues have rarely, if ever, surfaced. However, this could change with the anticipated surge of corporate bankruptcy resulting from the recent COVID-19 pandemic.[4] Going forward, bankruptcy judges and "consumer privacy ombudsmen" (CPOs) should be ever more mindful of the complex consumer-privacy legal landscape and increasingly vocal call for stricter standards related to the collection, use and transfer of consumer information across the nation.

Background

The current framework for dealing with the sale of consumer data in bankruptcy dates back to the dot-com crash of the early 2000s. In 2001, Toysmart.com, an online retailer of children's toys, sought to sell its assets, including its customer databases, under a chapter 11 liquidation plan, despite having promised customers that it would "never" share customer data with third parties. The Federal Trade Commission (FTC) objected to the sale[5] and eventually entered into a settlement with the debtor under which Toysmart could sell the customer data under the following conditions:

> (a) the buyer is engaged in substantially the same general line of business as the debtor;
> (b) the data would be sold as part of a larger group of assets, including intellectual property and goodwill;
> (c) the buyer must agree to treat the customer data in accordance with the debtor's applicable privacy policy; and
> (d) consumers must affirmatively consent to any material change in the governing privacy policy.[6]

Toysmart was unable to find a purchaser willing to agree to these conditions, and one of its equity

1 Robin Kurzer, "The Story of Data: How Did We Get Here?," *MarTech* (May 8, 2018), *available at* martechtoday.com/the-story-of-data-how-did-we-get-here-215146 (unless otherwise specified, all links in this article were last visited on May 26, 2020).

2 Louise Matskais, "The *WIRED* Guide to Your Personal Data (and Who Is Using It)," *WIRED* (Feb. 15, 2019), *available at* wired.com/story/wired-guide-personal-data-collection.

3 After the California Consumer Privacy Act passed in 2018 (AB No. 375, *available at* leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (last visited June 9, 2020), multiple states have proposed similar legislation to protect consumers in their states. As of April 16, 2020, two additional states have already enacted consumer-privacy legislation, and such legislation has been introduced and/or is under consideration in 24 others. Mitchell Noordyke, "U.S. State Comprehensive Privacy Law Comparison," IAPP, *available at* iapp.org/resources/article/state-comparison-table/ (last visited June 9, 2020).

4 ABI's Coronavirus Resources for Bankruptcy Professionals website (abi.org/covid19) aggregates information for bankruptcy professionals to assist clients and provide guidance due to the fallout from the COVID-19 pandemic.

5 *See* First Amended Complaint, *FTC v. Toysmart.com Inc.*, No. 00-11341 (D. Mass. July 21, 2000), Dkt. 2.

6 Stipulated Consent Agreement and Final Order, *In re Toysmart.com LLC*, No. 00-13995-CJK (Bankr. D. Mass. July 21, 2000), Dkt. 113; *see* Consumer Privacy Ombudsman Report ¶ 32, *In re BPS US Holdings Inc.*, No. 16-12373 (Bankr. D. Del. Jan. 19, 2017), Dkt. 593 (summarizing *Toysmart* settlement).

owners purchased the data for $50,000 and destroyed it prior to Toysmart's formal dissolution.[7]

The Code PII Provisions

The *Toysmart* case prompted congressional action.[8] In 2005, Congress amended the Bankruptcy Code to include provisions protecting the sale of "personally identifiable information" (PII) as set forth below (collectively the "Code PII provisions").

Section 363(b)(1) of the Bankruptcy Code governs sales of PII by providing that a bankruptcy court may approve the debtor's transfer of PII, notwithstanding "a policy prohibiting the transfer" of such PII, if the court, after the appointment of a CPO and notice and hearing, approves the sale (1) "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."[9]

Section 101(41A) of the Bankruptcy Code defines PII to include a consumer's name, address, email address, telephone number, Social Security number, credit card number and "any other information concerning an identified individual that, if disclosed, will result in contacting or identifying such individual physically or electronically."[10] However, PII is limited to information "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." Section 332 of the Bankruptcy Code outlines the role of the CPO, who "shall provide to the court information to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale" of PII, including:

> (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.[11]

The CPO was created expressly to advise bankruptcy courts regarding a debtor's existing privacy policies and its standards regarding certain consumer data sales and transfers. In this way, the CPO's role was also created to protect consumer-data privacy.

Since the Code PII provisions were enacted, there have been several dozen cases where a CPO has been appointed and filed a report.[12] In these cases, the debtor will often accept the CPO's recommendations or negotiate protections with the U.S. Trustee and other parties-in-interest. A number of PII sales have drawn strong opposition from the FTC, state attorneys general and other creditors.[13] A debtor will typically modify the sale terms to assuage the concerns of the objecting parties. These negotiated outcomes are generally consonant with the *Toysmart* framework.[14] Courts will require a data sale to be combined with a sale of the debtor's other assets, to a purchaser in the same line of business, and in adherence to the debtor's privacy policy as of the petition date. These protections at least implicitly preclude data brokers from the pool of eligible purchasers in sales subject to the Code PII provisions. Courts may require a notice to affected consumers and provide them with an opportunity to opt out of the sale or otherwise limit the use of their data. However, it is important to note what the Code PII provisions do not address.

> **[T]he express provisions of the existing Bankruptcy Code seem to tie the hands of the courts from extending protections to consumers whose data has been collected, analyzed, profiled and otherwise used by companies.**

First, the Code PII provisions only concern sales that are prohibited under a debtor's privacy policy. Section 363(b)(1) is triggered upon a transfer in violation of a policy prohibiting the transfer of PII. If a policy permits the transfer of consumer data, such transfer may proceed in bankruptcy.

Second, the PII provisions only govern data collected by the debtor from a consumer. Companies collect information in countless ways and from different sources over time. These days, a vast amount of the consumer information held by businesses originally came from third-party data collectors whose sole function is to compile information on more than 700 million people from other public and private sources.[15] For example, employers collect PII from employees, companies may purchase lists from data brokers, and companies may obtain information about an individual through third-party cookies and other relationships. None of this is covered by the Code PII provisions, which are limited to information "provided by an individual to the debtor in connection with obtaining a product or a service

7 *See* Consumer Privacy Ombudsman's Report ¶ 46, *In re Bon-Ton Stores Inc.*, No. 18-10248 (Bankr. D. Del. Sept. 6, 2018), Dkt. 1062.

8 Opening Floor Statement of Sen. Patrick Leahy on the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, S. 256, Feb. 28, 2005.

9 11 U.S.C. § 363(b)(1).

10 Section 101(41A) provides in full: "Personally identifiable information" means:

> (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 one 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.

11 11 U.S.C. § 332(b).

12 Bon Ton CPO Report at ¶ 62 (collecting cases).

13 *See* Debtors' Consolidated Reply in Support of IP Sale, *In re RadioShack Corp.*, No. 15-10197 (Bankr. D. Del. May 19, 2015), Dkt. 2178 (addressing objections from dozens of state attorneys general, FTC, Apple, Verizon and AT&T); Lucy L. Thomson, "Personal Data for Sale in Bankruptcy: A Retrospective on the Consumer Privacy Ombudsman," XXXIV *ABI Journal* 6, 32-33, 80-81, June 2015, *available at* abi.org/abi-journal (collecting cases).

14 *See* Report of the Consumer Privacy Ombudsman at 8, *In re RadioShack Corp.*, No. 15-10197 (Bankr. D. Del. May 16, 2015), Dkt. 2148 ("In broad terms, [CPOs] have recommended, and Bankruptcy Courts have approved, the sale of PII in contravention of a debtor's existing privacy policy; provided that: (i) the sale is made to a 'Qualified Buyer;' (ii) the purchaser is the successor-in-interest to the debtor's privacy policy; and (iii) consumers are afforded notice of the proposed sale and given an opportunity to opt out of the proposed transfer of PII.").

15 *See* Thomson, *supra* n.13 (collecting cases).

from the debtor primarily for personal, family, or household purposes." In short, the Code PII provisions are outdated and do not reflect how businesses in the digital age collect information about consumers, and thereby leave potentially huge openings for the unmonitored sale or transfer of consumer information in bankruptcy proceedings.

In light of these two gaps, there may never be a more critical time for bankruptcy courts to appoint a CPO than today to safeguard the privacy of consumer data and ensure that any proposed sale in bankruptcy does not violate applicable nonbankruptcy laws, regulations or industry standards. Yet the law might not provide courts with the tools to do so, because the current Code PII provisions are only triggered if the transfer would violate an existing privacy policy.

For example, imagine a data broker who scours chapter 11 cases looking for data to collect and build its database. What about companies whose data-privacy policies are inconsistent with the debtor's data-privacy policies with respect to the circumstances under which PII will be shared or sold, where the purchaser of the consumer data will now use consumer data in a way that an individual *never* anticipated it would be used when providing the information in the first instance? For example, what if the debtor did not provide information to advertising companies, but the purchaser of the PII does so on a regular basis and discloses that fact in their privacy policy? As we stand on the precipice of what is expected to be a wave of bankruptcy sales and liquidations, notions of how to responsibly and ethically handle consumer PII — and not just as that term is defined in the Code PII provisions — will be tested.

Changes Ahead?

The Code PII provisions have yielded no meaningful decisional authority, and there are no reported decisions involving a contested sale of PII under § 363(b). As restructuring professionals anticipate a new wave of bankruptcies, it is likely the Code PII provisions will be tested in a way they have not been before.

Statutory Framework Is Flexible

Although PII sales have generally followed the *Toysmart* framework for the last two decades, the Bankruptcy Code does not incorporate this framework. The only requirements for a sale of PII that is prohibited by a debtor's privacy policy are (1) the appointment of a CPO; (2) the bankruptcy court's "due consideration to the facts, circumstances, and conditions" of such transfer after notice and hearing; and (3) compliance with applicable nonbankruptcy law.

Suppose the debtor is AppCo, which operates a food-delivery app that tracks its users' movements and web-browsing history. The debtor's privacy policy states that it will not use geolocation data to provide advertisements. This data could be used to identify the consumer and constitutes "personally identifiable information."[16] AppCo has no hope for reorganization and must liquidate.

If AppCo attempts to sell the consumer data to another company engaged in a substantially similar business (*i.e.*, another food-delivery app) with other assets, and the purchaser agrees to abide by AppCo's privacy policy, a court would likely approve the sale in accordance with *Toysmart*. However, what if the only bidder is a data broker or another company offering a different service that wants to aggregate AppCo's data and use it for purposes that were not disclosed to AppCo consumers, such as using the geolocation data for marketing purposes? The CPO would likely recommend against the sale as violating the consumers' expectations of privacy, and the U.S. Trustee and state attorneys general would likely oppose the sale. What if the broker offered a price that would pay all of the debtor's creditors in full, and rejecting its offer would leave creditors with little or no recovery?

The court may ultimately approve a sale after "giving due consideration to the facts, circumstances, and conditions of such sale."[17] In effect, the Bankruptcy Code directs a bankruptcy court to weigh the recovery to the estate against the privacy interests of consumers. There is substantial discretion on the part of a bankruptcy judge to approve sales of consumer data that would violate a debtor's privacy policy. The Code PII provisions were enacted to protect consumer privacy, and bankruptcy courts will generally be loath to sacrifice privacy solely to maximize creditor recovery. However, if the bankruptcy court determines that harm to consumer privacy is modest, it might approve a contested sale.

Is the Data PII?

There might be questions about whether the data at issue falls within the contours of the Code PII provisions. What should courts do with lists purchased, or information collected from third parties? Is there a way to include what we commonly consider PII in today's world in the Code PII provisions despite a lack of express authority? To address this obvious gap in the existing Code PII provisions, bankruptcy courts might look to their equitable powers to sweep in data of this kind. Indeed, even if the data is not considered PII, a bankruptcy court likely has authority to appoint a CPO to opine on a proposed sale's compliance with applicable nonbankruptcy law and its effect on consumer privacy. Bankruptcy courts have expanded on their statutory authorizations to appoint officers or professionals at the expense of the estate when the court feels that input from independent third parties would be beneficial.[18]

Conclusion

Given the impact of the COVID-19 pandemic, the harsh reality is that many companies will seek restructuring or liquidation protection. In today's digital world, *every one* of those companies has what would commonly be considered PII, whether it is a simple email list or more sophisticated consumer databases. Yet the express provisions of the existing Bankruptcy Code seem to tie the hands of the courts from extending protections to consumers whose data has been collected, analyzed, profiled and otherwise used by companies.

Nonetheless, the need to facilitate debtor rehabilitation should not necessarily outweigh a consumer's implicit (or

16 *See* 11 U.S.C. § 101(41A)(B)(ii).

17 11 U.S.C. § 363(b)(1)(B)(i).

18 *Collier on Bankruptcy* ¶ 332.02 (Richard Levin & Henry J. Sommers eds., 16th ed. 2020).

explicit in some states) right to privacy. At a minimum, a debtor should be required to provide notice to its customers of the pending PII transfer in a bankruptcy sale, and, in some circumstances, obtain the customer's opt-in or opt-out consent to the sale.

Furthermore, certain legislative action could strengthen consumer privacy within the bankruptcy courts, such as amending the language of §§ 322 and 363 to provide CPOs with more authoritative oversight in cases where consumer information is transferred, reducing the bankruptcy court's broad discretion. The Bankruptcy Code could also be amended to require the appointment of a CPO in any case where a debtor is likely to sell consumer information, even in cases where a purchaser agrees to abide by the debtor's existing privacy policy and it appears that there is no conflict. The authors anticipate that while the CPO provisions have not led to any reported decisions to date, the scope of the authority of that ombudsman is about to become central to the coming wave of restructuring as courts look to appoint CPOs, even when the Code PII provisions might not expressly permit or require such appointment. abi

Reprinted with permission from the ABI Journal, Vol. XXXIX, No. 7, July 2020.