THE SALE OF PERSONALLY IDENTIFIABLE INFORMATION IN BANKRUPTCY

MICHAEL ST. PATRICK BAXTER*

TABLE OF CONTENTS

INTRODUCTION

In a digital economy, information can be more valuable than tangible assets.[1] One of a business debtor's more valuable assets is the personal information it has collected from its customers.[2] This information may include names, physical addresses, e-mail addresses, telephone numbers, purchase histories, personal preferences, and many other types of information. Personal information about consumers is highly valued, as businesses and marketers increasingly seek ways to target consumers with specific demographics and interests.[3]

When a debtor wishes to sell the personal information it has collected from consumers, a tension is created between the debtor's interest in maximizing the value of its assets and the consumers' interest in privacy.[4] If the debtor's privacy policy prohibits the sale of its customers' personal information or if the privacy policy fails to disclose that the debtor may sell or transfer such information to third

---

 Partner, Covington & Burling LLP; Professorial Lecturer in Law, The George Washington University Law School; Conferee, National Bankruptcy Conference; Fellow, American College of Bankruptcy; Founding Member, International Insolvency Institute; and Member, The American Law Institute. The author was the consumer privacy ombudsman in the Borders and BPS Holdings bankruptcy cases. I am grateful for the valuable comments on an earlier draft of this article from Rachel A. Greenleaf, David J. Bender, Julia C. Duke, and Joan S. Baxter. The views expressed are solely those of the author.

[1] *See* Kayla Siam, *Coming to a Retailer Near You: Consumer Privacy Protection in Retail Bankruptcies*, 33 EMORY BANKR. DEV. J. 487, 491 (2017) ("While tangible assets tend to deflate in value over time, intangible assets, such as consumer information, tend to increase in value . . . .").

[2] *See* Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 779, 783, 788 (2001) (describing the type of information a business may extract from a given customer's actions and how that information can help a business target its advertising).

[3] *See* Siam, *supra* note 1, at 502–03 ("[C]ompanies use personal information to efficiently market products and services to consumers . . . .").

[4] *See* Daniel Brian Tan, *Maximizing the Value of Privacy Through Judicial Discretion*, 34 EMORY BANKR. DEV. J. 681, 681 (2018) (explaining the increased risk of breaching consumer confidentiality when a business collects PII).

parties, the Bankruptcy Code[5] requires that a consumer privacy ombudsman be appointed to assist the bankruptcy court in its consideration of the proposed sale.[6] Less clear is whether the appointment of a consumer privacy ombudsman is determined solely by the version of the debtor's privacy policy in effect on the date of bankruptcy or whether there are circumstances in which a court may consider a debtor's previous privacy policies. In other words, is the debtor's privacy policy in place on the petition date the only privacy policy that matters in a sale of personal information? The answer to this question is critical because it may determine whether the appointment of a consumer privacy ombudsman is required, and whether the personal information can even be sold in the first place.

The Federal Trade Commission ("FTC") has made it clear that a debtor's privacy policy on the petition date is not the only privacy policy that matters.[7] There are circumstances in which the personal information collected by the debtor may be subject to representations in prior privacy policies.[8] For example, if a consumer has submitted personal information pursuant to a privacy policy that either prohibits its sale or fails to disclose that such information may be sold or transferred, the consumer's information may not be sold unless the consumer has consented to any subsequent change in the privacy policy to permit such a sale.[9] If the consumer has not consented to any subsequent change in the privacy policy, the consumer's personal information may continue to be governed by the privacy policy in place at the time his or her personal information was submitted or collected.[10]

This article will address the Bankruptcy Code's requirements for a debtor's sale of personally identifiable information in bankruptcy. Part I will review the requirements when the debtor's privacy policy on the petition date prohibits the proposed sale. Part II will discuss the *Toysmart* conditions that continue to serve as the template for the sale of personal information in violation of an applicable

---

[5] *See* 11 U.S.C. § 101(41A) (2012) (enumerating what constitutes personally identifiable information in bankruptcy).

[6] *See id.* § 363(b)(1)(B) (outlining the scenarios in which a consumer privacy ombudsman is necessary).

[7] *See, e.g.*, Complaint at 5–6, *In re* Gateway Learning Corp., FTC Docket No. C-4120 (F.T.C Sept. 10, 2004) (alleging a violation of section 5 of the FTC Act when a company retroactively applied material changes to a privacy policy to personal information collected under a prior privacy policy); *see also* Jamie Hine, *Mergers and Privacy Promises*, FTC: BUS. BLOG (Mar. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises ("Simply revising the language in a privacy policy or user agreement isn't sufficient because existing customers may have viewed the original policy and may reasonably assume it's still in effect.").

[8] *See* Complaint, *supra* note 7, at 5–6 (contending that retroactively applying a revised privacy policy, which allowed the sharing of personally identifiable information with third parties, to information collected by consumers under a prior privacy policy, which expressly disallowed such sharing of information, constituted "unfair and deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act").

[9] *See id.* (arguing that respondent violated section 5(a) of the FTC Act because respondent changed its privacy policy without notifying consumers).

[10] *See* Hine, *supra* note 7 (explaining that, for a company to alter privacy promises already made by them to consumers, it must inform the consumers and receive their express, affirmative consent to opt-in to the company's new privacy practices).

privacy policy.[11] Part III will discuss the Bankruptcy Code's requirements when the privacy policy on the petition date permits the proposed sale, but a prior, still applicable privacy policy prohibits the sale.

I. PII AMENDMENTS TO THE BANKRUPTCY CODE

Over a decade ago, Congress addressed the privacy of personal information in bankruptcy sales in the 2005 amendments to the Bankruptcy Code.[12] To protect consumers when a debtor proposes to sell their personal information, section 363(b)(1) of the Bankruptcy Code was amended to impose conditions on the sale of personally identifiable information ("PII") if the debtor has a privacy policy "in effect on the date of the commencement of the case" that prohibits the transfer of PII.[13] Contemporaneously with the amendment of section 363(b)(1), Congress added the definition of PII to the Bankruptcy Code.[14] PII is defined to include an individual's name, physical address, electronic address, telephone number, social security number or credit-card number, as well as any other information that can be

---

[11] *See FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations*, FTC: PRESS RELEASES (July 21, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding [hereinafter *FTC Announces Settlement with Toysmart*] (stating when customer information is to be sold in violation of a privacy agreement, it may not be sold as a stand-alone asset and may only be sold as part of a package which includes the entire website, and that the package may only be sold to a "qualified buyer").

[12] *See* Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, Pub. L. No. 109-8, § 231, 119 Stat. 23, 72–73 (2005) (amending section 363(b)(1) of title 11 of the United States Code to include restrictions on a debtor's ability to transfer PII when a policy exists that prohibits its transfer).

[13] 11 U.S.C § 363(b)(1) (2012).

[14] *See id.* § 101(41A). Section 101(41A) provides:

> The term "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 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.

Id.

combined with any of the foregoing items of information to facilitate identifying or contacting the individual.[15]

If, on the petition date, the debtor has a privacy policy that prohibits the sale or transfer of PII (or, a privacy policy that fails to disclose that the debtor may sell or transfer PII, and therefore impliedly prohibits such a sale or transfer), the debtor may sell the PII only if one of the following two conditions is satisfied: (1) the sale is consistent with the debtor's privacy policy in effect on the date of the commencement of the case; or (2) a consumer privacy ombudsman is appointed and the bankruptcy court approves the sale after finding the absence of any showing that the sale would violate applicable nonbankruptcy law.[16] Thus, a consumer privacy ombudsman must be appointed when the debtor's privacy policy in effect on the date of the commencement of the case prohibits the proposed sale of PII or fails to disclose that the debtor may sell PII to third parties, thereby impliedly prohibiting such a sale.[17]

Once appointed, the role of the consumer privacy ombudsman is to provide the bankruptcy court with information, usually in the form of a report, to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale of PII.[18] If a consumer privacy ombudsman is required, the bankruptcy court must

---

[15] *See id.*

[16] *See id.* § 363(b)(1). 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.

Id.

[17] *See id.*

[18] *See id.* § 332(b). Section 332(b) provides:

> 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

order the United States Trustee ("U.S. Trustee") to appoint an ombudsman no later than seven days before the sale hearing.[19] Seven days does not allow much time for an ombudsman to act, so it is wise for the U.S. Trustee to appoint an ombudsman once it becomes apparent that PII may be sold in violation of an applicable privacy policy.[20] The ombudsman may appear at the sale hearing and provide the court with information, including the debtor's privacy policy, the potential privacy harms or gains to consumers if the sale were approved, the costs and benefits of the sale to consumers, and any potential alternatives that might mitigate privacy losses or potential costs to consumers.[21]

If the debtor's privacy policy prohibits the proposed sale of PII or fails to disclose that the debtor may sell PII to third parties, the consumer privacy ombudsman will so advise the court.[22] In many cases, the ombudsman will suggest ways in which the sale may be accomplished consistent with the applicable privacy policy, or ways to address privacy concerns or to mitigate privacy harms.[23] The suggestions of the consumer privacy ombudsman are often accepted by the debtor,[24] in which case, the bankruptcy court will usually approve the sale of PII, subject to

---

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

Id.

[19] *See id.* § 332(a).

[20] *See* Objection of the United States Trustee to Debtors' Motion for Entry of (I) An Order (A) Approving Bidding Procedures and Bid Protections in Connection with the Sale of Certain Assets Related to the Business of Quirky, Inc., (B) Approving Procedures for Assumption and Assignment of Executory Contracts, (C) Approving the Form and Manner of Notice, and (D) Scheduling an Auction and a Sale Hearing, and (II) An Order Authorizing and Approving the Sale of Assts [sic] of Quirky, Inc. at 5, *In re* Quirky, Inc., No. 15-12596 (Bankr. S.D.N.Y. Oct. 7, 2015) [hereinafter Obj. to Debtors' Mot.] (serving as an example of prompt appointment of a consumer privacy ombudsman after the U.S. Trustee realized a proposed sale would violate a prior, but still applicable, privacy policy).

[21] *See* 11 U.S.C. § 332(b).

[22] *See, e.g.*, Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman at 46, *In re* Borders Group, Inc., 462 B.R. 42 (Bankr. S.D.N.Y. Dec. 7, 2011) (No. 11-10614) ("Debtor cannot transfer to Buyer any consumer's purchase history information that includes the title, genre and other details about specific audiovisual materials . . . regardless of when it was collected, unless Debtor obtains the written consent of the affected consumer.").

[23] *See, e.g.*, Second Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman at 49**,** *In re* Old BPS US Holdings, Inc., No. 16-12373 (Bankr. D. Del. Feb. 1, 2017) (suggesting that the proposed sale is consistent with the privacy policy as long as the Debtor provides consumers with notice of the transfer); *see also* Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman, *supra* note 22, at 46 (recommending that debtor may transfer PII to buyer so long as the debtor obtains the affirmative consent of affected consumers).

[24] This is a prudent action by the debtor because it will usually facilitate a smoother sale of PII. But sometimes the buyer takes exception to the ombudsman's suggestions. *See, e.g.*, Suppl. Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman at 3, *In re* Borders Group, Inc., 462 B.R. 42 (Bankr. S.D.N.Y. Dec. 7, 2011) (No. 11-10614) (discussing the buyer disagreed with the ombudsman's report and declined to follow certain suggestions for the sale, which resulted in a *sua sponte* hearing before the court and a second notice by the buyer to consumers in order to correct the buyer's first, deficient notice).

the conditions proposed by the consumer privacy ombudsman and agreed to by the debtor.[25]

In addition to ensuring compliance with the debtor's privacy policy, the consumer privacy ombudsman must determine if the proposed sale would violate applicable nonbankruptcy law.[26] Some federal laws that may apply to the sale of PII include the Children's Online Privacy Protection Act[27] ("COPPA") for children's information, the Health Insurance Portability and Accountability Act[28] for medical information, and the Gramm-Leach-Bliley Act[29] when the debtor provides financial services.[30] State laws may also be applicable, depending on the location of the consumers whose PII is being sold.[31] Even certain international laws may be applicable, to the extent they apply extraterritorially to U.S. companies. For instance, the European Union ("EU") General Data Protection Regulation ("GDPR") applies in some circumstances to the processing of personal data of EU data subjects, even if that processing occurs outside the EU.[32]

---

[25] *See, e.g.*, Second Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman, *supra* note 23, at 50 (proposing conditions rendering the sale of PII consistent with the applicable privacy policy, such as providing consumers with notice of the transfer). In *In re* Borders Group, after the consumer privacy ombudsman reported that the sale of PII would violate the debtor's privacy policies, the Judge asked the ombudsman to work with the debtor, the FTC, various states' attorneys general, and other parties in interest to reach a negotiated solution to address the privacy concerns, which led to a negotiated sale order. *See* Order re Suppl. Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman at 1, *In re* Borders Group, Inc., 462 B.R. 42 (Bankr. S.D.N.Y. Dec. 7, 2011) (No. 11-10614).

[26] *See* 11 U.S.C. § 363(b)(1) ("[T]he trustee may not sell or lease personally identifiable information to any person unless—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—finding that no showing was made that such sale or such lease would violate applicable nonbankruptcy law.").

[27] *See generally* 15 U.S.C. §§ 6501–6505 (2012).

[28] *See, e.g.*, 42 U.S.C. § 1320(d-6)(b) (2012). The United States Code explicitly prohibits the sale of individually identifiable health information "for commercial advantage, personal gain, or malicious harm." *Id.*

[29] *See generally* 15 U.S.C. §§ 6801–6827.

[30] *See* Ieuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS PRAC. LAW 1, 3 (2017), https://1.next.westlaw.com/Browse/Home/PracticalLaw?transitionType=Default&contextData=(sc.Default)&tabName=Practice Areas ("There are already a panoply of federal privacy-related laws that regulate the collection and use of personal data. Some apply to particular categories of information, such as financial or health information, or electronic communications.").

[31] *See, e.g.*, CAL BUS. & PROF. CODE § 22575 (West, Westlaw through Ch. 613 of 2018 Reg. Sess.). California also recently enacted the California Consumer Privacy Act ("CCPA"), which is the most comprehensive data privacy statute in the United States and introduces significant new privacy requirements on covered businesses. *See generally* A.B. 375, 2018 Cal. Legis. Serv. Reg. Sess. (Cal. 2018). The CCPA does not take effect until 2020. *Id.*

[32] *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing *Directive 95/46/EC* (General Data Protection Regulation), 2016 O.J. (L 119) 1, 31 [hereinafter Regulation 2016/679](indicating if a United States company has an "establishment" in the EU, offers goods or services to EU data subjects, or "monitors" the behavior of such data subjects, the GDPR would apply to that company's processing of personal data even if that processing occurs in the United States).

The most commonly applicable nonbankruptcy law is the Federal Trade Commission Act[33] ("FTC Act"). The FTC may commence enforcement actions against a company that fails to comply with the company's own posted privacy policies and for the unauthorized disclosure of consumer information as "unfair and deceptive practices" in violation of the FTC Act.[34] Therefore, the FTC Act may be relevant in any sale of PII that is inconsistent with a debtor's privacy policy. In addition, many states have their own counterpart to the FTC Act that authorizes the states to take similar enforcement actions.[35]

II. THE *TOYSMART* TEMPLATE

The Toysmart.com, LLC ("Toysmart") bankruptcy in 2000 created the template for the sale of PII in the face of a privacy policy prohibiting such a sale.[36] Toysmart was an online business that sold children's toys.[37] In the course of its business, Toysmart collected the personal information of visitors to its website, including names, addresses, billing information, and children's birthdates.[38] Toysmart collected this personal information pursuant to a privacy policy that stated that the information would "never" be shared with third parties.[39] Once in bankruptcy, however, Toysmart attempted to sell all of its assets, including its detailed customer databases.[40] The FTC brought an action against Toysmart for injunctive relief to prevent the sale of the customer data in violation of the privacy policy.[41] The FTC

---

[33] *See* 15 U.S.C. §§ 41–58 (creating the FTC and codifying provisions to protect consumers and increase business transparency by working to prevent anticompetitive, deceptive, and unfair business practices).

[34] *See* Jolly, *supra* note 30, at 3 (highlighting the FTC commonly brings enforcement actions against companies that make unauthorized disclosures of personal information in violation of the companies' own posted privacy policies).

[35] *See, e.g.*, 815 ILL. COMP. STAT. ANN. § 505/2 (West, Westlaw through Pub. Acts 100-1114, of the 2018 Reg. Sess.) (stating Illinois's Consumer Fraud and Deceptive Business Practices Act declares "unfair methods of competition and unfair or deceptive acts or practices, . . . with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any [deceptive practice] . . . in the conduct of any trade or commerce . . . unlawful[,]" and noting the FTC Act and relevant federal case law should be used in "construing" the provisions).

[36] *See* FEDERAL TRADE COMMISSION, PRELIMINARY FTC STAFF REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 8–9 n.17 (2010) (discussing *Toysmart* as one of several cases involving deceptive statements in companies' privacy notices about the collection and use of consumer data).

[37] *See FTC Announces Settlement with Toysmart*, *supra* note 11 (describing Toysmart as "a popular Web site that marketed and sold educational and non-violent children's toys over the Internet").

[38] *See id.* (restating the type and variety of customer data Toysmart collected).

[39] *See* Complaint for Permanent Injunction and Other Equitable Relief at Ex. 1, Fed. Trade Comm'n v. Toysmart.com, Inc., No. 00-11341 (D. Mass. July 23, 2004) ("Personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party.").

[40] *See id.* at 4 (alleging "Toysmart has disclosed, sold, or offered for sale its customer lists and profiles").

[41] *See id.* at 5 (requesting the court grant an injunction against Toysmart for violating the FTC Act); *see also FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors*, FTC: PRESS RELEASES (July 10, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/ftc-sues-failed-website-toysmartcom-deceptively-offering-sale.

alleged that the sale constituted an "unfair or deceptive act" in violation of section 5(a) of the FTC Act.[42]

The FTC action against Toysmart was settled.[43] Under the terms of settlement, the FTC allowed Toysmart to sell its customer information in the bankruptcy proceeding on the following conditions: (1) the customer information was sold as part of a package with the debtor's other assets; (2) the buyer was in the same line of business as the debtor (referred to as a "qualified buyer"); (3) the buyer agreed to comply with Toysmart's privacy policy with respect to the purchased customer information; and (4) the buyer notified the affected customers and obtained their affirmative consent before using their personal information for any new uses.[44]

Although *Toysmart* preceded the addition of the PII provisions to the Bankruptcy Code, the *Toysmart* conditions continue to serve as the template for the sale of PII in violation of an applicable privacy policy.[45] If PII is proposed to be sold to a buyer in substantially the same line of business as the debtor, it is usually sufficient if the affected consumers are notified of the sale—often by a direct email and a posting on the website—and given an opportunity to opt out of having their PII transferred to the buyer.[46] If the buyer is not in substantially the same line of business as the debtor, the court may still approve the sale of PII if the affected consumers affirmatively consent or opt in to the sale (as opposed to merely being given an opportunity to opt out).[47]

III. PRIOR PRIVACY POLICIES

But what if, prior to bankruptcy, the debtor had changed its privacy policy from a policy that either prohibited the sale of PII or failed to disclose that the debtor may

---

[42] *See* First Amended Complaint for Permanent Injunction and Other Equitable Relief at 2, 5, Fed. Trade Comm'n v. Toysmart.com, LLC, No. 00-11341 (D. Mass. July 23, 2004). The complaint also alleged that Toysmart kept the information of children under the age of 13 in violation of COPPA. *See id.* at 5.

[43] *See FTC Announces Settlement with Toysmart*, *supra* note 11 (highlighting the settlement demonstrates the FTC's commitment to enforcing COPPA and ensuring that websites that retrieve information from children 13 and under comply with parental notification requirements).

[44] *See id.* The settlement also required Toysmart to delete or destroy any customer data in the event the bankruptcy court did not approve the sale. *See id.* In addition, any information kept in violation of COPPA had to be destroyed. *See id.*

[45] *See, e.g.*, Letter from Jessica L. Rich, Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Frejka PLLC, at 5 (May 16, 2015), https://www.ftc.gov/system/files/documents/public_statements/643291/150518radioshackletter.pdf. The *Toysmart* conditions were recommended by the consumer privacy ombudsmen and/or adopted in the sale of PII by Radioshack, Borders, Golfsmith, and Adinath Corp. *See* Report of the Consumer Privacy Ombudsman at 19, *In re* Golfsmith Int'l Holdings, Inc., No. 16-12033 (Bankr. D. Del. Oct. 28, 2016); *see also* Report of the Consumer Privacy Ombudsman, *In re* Adinath Corp. Simply Fashion Stores LTD., No. 15-16888 (Bankr. S.D. Fla. July 29, 2015); Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman, *supra* note 22, at 26–27.

[46] *See, e.g.*, Report of the Consumer Privacy Ombudsman, *In re* Golfsmith Int'l Holdings, Inc., *supra* note 45 at 2 (explaining the buyer in this case agreed to provide notice to customers, giving them the opportunity to opt-out from having their PII transferred to the buyer).

[47] *See id.* at 4 (explaining an entity that is not a qualified buyer must agree to abide by debtors' existing privacy policy and provide customers with the opportunity to opt-in to the transfer, otherwise customer PII will not be transferred).

sell PII to third parties, to a less restrictive policy expressly permitting the sale of PII? As technology has evolved and personal information has become more valuable, so too have privacy policies evolved. Since *Toysmart*, many companies have revised their privacy policies to permit the sale, transfer, or other disposition of personal information in the event of bankruptcy, in addition to much broader circumstances (*e.g.*, any corporate transaction), not limited to bankruptcy.[48]

For well-established companies, it is common for their privacy policies to have changed over time, including in response to developments in privacy and data-protection laws.[49] At the dawn of the digital era, a company's first privacy policy pursuant to which it collected personal information was probably very restrictive and, like Toysmart, may have provided that the company would never disclose the collected information to any other person.[50] Such a policy may have been necessary at the time to persuade consumers to share their personal information, and perhaps the value of the information was not recognized. As the value of personal information became more apparent and consumers became less reluctant to share their personal information, the same company may have changed its privacy policy to a less restrictive form. It may have adopted a privacy policy that the company will not disclose, sell, or transfer personal information to any person without the affirmative consent of the consumer. Fast-forward to today, and the company's privacy policy may have changed several more times to give the company the right to disclose, sell, or transfer the personal information under any circumstances, perhaps even without the affirmative consent of the consumer. Companies also commonly revise privacy policies in response to changing legal requirements. Many United States companies, for instance, updated their privacy policies to comply with enhanced notice obligations under the GDPR.[51]

As discussed above, the appointment of a consumer privacy ombudsman is only required if the proposed sale is inconsistent with the debtor's privacy policy "in effect on the date of the commencement of the case."[52] If the proposed sale violates

---

[48] *See, e.g., Privacy Policy*, THE WASHINGTON POST (May 24, 2018), https://www.washingtonpost.com/privacy-policy/2011/11/18/gIQASIiaiN_story.html ("We reserve the right to transfer any information we have about you in the event that we sell or transfer all or a portion of our business or assets to a third party, such as in the event of a merger, acquisition, or in connection with a bankruptcy reorganization."); *see also Walmart Privacy Policy*, WALMART (updated Nov. 2017), https://corporate.walmart.com/privacy-security/walmart-privacy-policy ("In the event that all or a part of our business is merged, sold or reorganized (including transfers made as a part of insolvency or bankruptcy proceedings), personal information about you could be shared with the successor business.").

[49] *See, e.g.*, Anick Jesdanun, *GDPR: Why You're Getting All Those Privacy Emails, and What's Changing Under New EU Rules*, THE CHICAGO TRIBUNE (May 25, 2018), http://www.chicagotribune.com/business/ct-biz-gdpr-privacy-rules-20180525-story.html (describing privacy policy changes to comply with new requirements under the GDPR).

[50] *See FTC Announces Settlement with Toysmart*, *supra* note 11 (explaining Toysmart's privacy policy stated information gathered from customers would never be shared with third parties).

[51] *See* Regulation 2016/679, *supra* note 32, at 40–41 (specifying a variety of disclosures required prior to collecting personal data); *see also* Jesdanun, *supra* note 49 (explaining the GDPR forces companies to: (1) disclose data breaches within 72 hours of their occurrence; (2) clarify how long they keep personal information and data; and (3) use plain language when explaining their process of gathering and using data).

[52] 11 U.S.C. § 363(b)(1) (2012).

the debtor's privacy policy, it is clear that a consumer privacy ombudsman must be appointed to review the sale, and that the sale must not violate applicable nonbankruptcy law.[53] In bankruptcy, some debtors may take the position—contrary to that of the FTC—that the only privacy policy that matters is the privacy policy in place on the date of the filing of the bankruptcy petition.[54] But, if the only privacy policy that matters is the privacy policy in place on the petition date, and, if that policy discloses (or at least does not prohibit) the possible sale of PII, such a sale would arguably be consistent with the debtor's privacy policy, and the Bankruptcy Code would not require the appointment of a consumer privacy ombudsman.[55] This would mean a debtor—even on the eve of bankruptcy—could change its privacy policy from one that prohibits the sale of PII, to one that permits the sale of PII without additional notice or affirmative consent.

Moreover, if the appointment of a consumer privacy ombudsman is not required, it is not clear that section 363(b)(1) would require the bankruptcy court to find that the proposed sale would not violate applicable nonbankruptcy law.[56] Still, it seems unlikely that a bankruptcy court would approve the sale of PII in the face of a violation of applicable nonbankruptcy law, even if the proposed sale was consistent with the debtor's privacy policy. However, in the absence of a consumer privacy ombudsman, it would fall to the U.S. Trustee to bring the matter to the attention of the bankruptcy court because it is unlikely that any party in interest would be willing to incur the personal expense of challenging the sale or the administrative expense of a consumer privacy ombudsman.

While the debtor's privacy policy on the petition date matters, it is not the only privacy policy that matters.[57] There are circumstances in which personal information collected by the debtor continues to be governed by representations in the debtor's prior privacy policies.[58] Consider a customer who has submitted

---

[53] *See id.* § 363(b)(1)(B)(ii) (stating the elements a trustee must fulfill to sell or lease PII to a third party).

[54] *See, e.g.*, Debtors' Motion for Entry of (I) An Order (A) Approving Bidding Procedures & Bid Prot. in Connection with the Sale of Certain Assets Related to the Bus. of Quirky, Inc., (B) Approving Procedures for Assumption & Assignment of Executory Contracts, (C) Approving the Form & Manner of Notice, & (D) Scheduling an Auction & a Sale Hearing & (II) An Order Authorizing & Approving the Sale of Assets of Quirky, Inc. at 21, *In re* Quirky, Inc., No. 15-12596 (Bankr. S.D.N.Y Oct. 1, 2015) [hereinafter Debtors' Mot. for Entry] (asserting consumer ombudsman is not necessary due to the presence of a privacy policy that allows the transfer of PII in connection with a merger, sale, reorganization, dissolution, or liquidation of the business).

[55] *See* 11 U.S.C. § 363(b)(1) (barring the use, sale, or leasing of a product or service that discloses PII if the debtor has offered a policy prohibiting transfer of such material, and that policy is in effect at the commencement of the case).

[56] *See id.* § 363(b)(1)(B) (requiring no showing that the sale would violate applicable nonbankruptcy law only if a consumer privacy ombudsman has been appointed).

[57] *See In re* Gateway Learning Corp., FTC Docket No. 042-0347, 2004 WL 2618647, at *5 (F.T.C. Sept. 10, 2004) (holding because the privacy policy had changed from the time the customer signed up with the company and there was no affirmative opt-in for the new policy, the company had to honor the previous policy).

[58] *See* Hine, *supra* note 7 (discussing language revisions to a privacy policy are not always sufficient because existing customers may reasonably assume the prior policy is still in effect, which ultimately binds those customers to that original privacy policy); *see also infra* notes 71–76 and accompanying text.

personal information pursuant to a privacy policy that prohibits the sale of the customer's personal information. Over time, the company may adopt various iterations of less restrictive privacy policies. If the customer has not consented (either expressly or impliedly) to any subsequent change in the privacy policy, the customer's personal information may continue to be governed by the privacy policy in place at the time the information was provided or collected.[59] This is likely the case for a one-time customer or a customer who has ceased to do business with the company. The FTC would likely view the sale of the PII of these one-time or past customers as "unfair and deceptive practices" in violation of the FTC Act.[60] Moreover, such a sale would violate section 363(b)(1) of the Bankruptcy Code because an earlier privacy policy, which is still applicable on the date of the commencement of the case, prohibits the sale.[61]

Consent may be implied. Indeed, certain website privacy policies state that the users consent to the company's privacy practices simply by using the websites governed by those privacy policies.[62]

However, if adequate notice of subsequent changes in the privacy policy was provided to the customer, it is possible that, as the privacy policy changes, the customer may have consented (either expressly or impliedly) to each change, so that the privacy policy governing the customer's personal information may in fact be the debtor's privacy policy in place on the petition date. When a customer continues to do business with the debtor after a change in the privacy policy, it may be that the customer has impliedly consented to the change in the privacy policy.[63] As a result, the terms of the new privacy policy may apply to the customer's personal information even though the information was submitted or collected under an earlier privacy policy that prohibited sale.

But for a customer who has never consented to a change in the privacy policy, the privacy policy that governs this customer's personal information is likely the privacy policy that was in place at the time the information was submitted or collected—not any subsequent privacy policy.[64] This is particularly so because the FTC requires companies to "obtain affirmative express consent prior to making

---

[59] *See infra* note 62 and accompanying text (explaining this consent may be implied).

[60] *See* Jolly, *supra* note 30, at 3.

[61] *See* 11 U.S.C. § 363(b)(1) ("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 . . . .").

[62] *See, e.g., Privacy Policy*, PERISCOPE (last visited Sept. 20, 2018), https://www.periscope.com/privacy-policy/ ("By using this Site, you consent to the processing of your personal information as described in this Privacy Notice."); *see also Slate's Privacy Policy*, SLATE (last visited May 22, 2018), https://slate.com/privacy ("By using the Services, you consent to the terms of this Privacy Policy and our Terms of Service.").

[63] *See supra* note 62 and accompanying text.

[64] *See* FEDERAL TRADE COMMISSION, PRELIMINARY FTC STAFF REPORT, *supra* note 36, at i–viii (explaining companies such as Google and Facebook are now required to obtain affirmative consent from customers before changing their privacy policies).

certain material retroactive changes to their privacy practices."[65] In other words, if a company seeks to apply materially different privacy practices to personal information collected under a prior privacy policy, it must obtain affirmative express consent prior to doing so to comply with FTC principles.[66] As a consequence, the debtor's database of PII may be governed by more than one, or perhaps even several, privacy policies, each of which may be materially different. This can create a problem if the debtor is unable to determine which specific privacy policy applies to which specific PII.

The text of the Bankruptcy Code supports the relevance of a debtor's prior privacy policy to the sale of PII. The requirement for the appointment of a consumer privacy ombudsman turns on whether the privacy policy "in effect on the date of the commencement of the case" prohibits the transfer of PII.[67] The privacy policy "in effect on the date of the commencement of the case" does not necessarily refer to the debtor's privacy policy in place on the petition date.[68] Instead, it refers to the privacy policy that applies to—or to use the statutory language, is "in effect" with respect to—the particular PII in question.[69] If, for the reasons discussed above, the debtor's PII is governed by more than one privacy policy, the appointment of a consumer privacy ombudsman is required if any applicable privacy policy—even if it is a prior privacy policy—prohibits the transfer of the PII in question.[70] This can be so even if the debtor's privacy policy on the petition date permits the sale of PII.[71] For consumers whose personal information was collected under an earlier, more restrictive privacy policy, and who did not consent to any subsequent privacy policy, the sale of their PII may violate the privacy policy applicable to their PII "in effect on the date of the commencement of the case."[72]

At least two bankruptcy cases illustrate the relevance of prior privacy policies to the sale of personal information in bankruptcy. In *In re Borders Group, Inc.*, the consumer privacy ombudsman addressed the difference in Borders Group Inc.'s ("Borders") changing privacy policies.[73] Originally, Borders had a privacy policy in

---

[65] *Id.* at 58.
[66] *See id.* at 57.
[67] 11 U.S.C. § 363(b)(1) (2012).
[68] *Id.*
[69] *See id.*
[70] *See id.* § 332(a); *see also* Order Pursuant to Sections 105, 363 & 365 of the Bankruptcy Code and Rules 2002, 6004 and 9014 of the Federal Rules of Bankruptcy Procedure Approving the Sale of Certain of the Debtors' IP Assets Free and Clear of All Liens, Interests, Claims and Encumbrances and the Rejection of Certain Executory Contracts Related Thereto at *5, *In re* Borders Group, Inc., No. 11-10614 (Bankr. S.D.N.Y Sept. 27, 2011) [hereinafter Order Approving Sale] (illustrating how the appointment of a consumer privacy ombudsman may be required when there are prior privacy policies).
[71] *See* Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman, *supra* note 22, at 19 (demonstrating an example of when an ombudsman was appointed even though the privacy policy on petition date permitted the sale of PII).
[72] *See id.* at 22 (stating since the sale was not consistent with earlier policies, it would only be permitted if it did not violate nonbankruptcy law).
[73] *See id.* at 19–22 (discussing the implementation of different privacy policies, which were "in effect" at the time the action was commenced).

place that required the affirmative consent of the customer before disclosing personal information to third parties.[74] In 2008, Borders revised its privacy policy to allow the company to disclose a customer's personal information if Borders needed to "sell, buy, merge or otherwise reorganize its own or other businesses."[75] The Borders consumer privacy ombudsman distinguished between the two privacy policies, stating that customer information collected prior to the 2008 privacy policy was governed by the prior privacy policy, which required more restrictive conditions on the sale of that information.[76]

With the assistance of the Borders consumer privacy ombudsman, the debtor, the official committee of unsecured creditors, various states' attorneys general, and other parties in interest agreed to a negotiated sale order that allowed the sale of PII—regardless of when the PII was collected—provided: (1) the buyer sent an email notice to each consumer whose PII was proposed to be transferred notifying them of the information to be transferred, explaining their PII will be subject to the buyer's privacy policy, and giving them 15 days to opt out of the transfer and to have their PII destroyed; (2) a notice of the transfer and opt-out right was posted for 30 days on the websites of both Borders and the buyer; and (3) the debtor publish a notice of the sale and opt-out right in *USA Today*.[77]

In *In re Quirky, Inc.*, the debtor sought to sell, among other assets, its database of 1.2 million community members and related PII.[78] The U.S. Trustee objected to the proposed sale on the grounds that a consumer privacy ombudsman was required because Quirky, Inc.'s ("Quirky") privacy policy prior to 2011 did not permit the sale of PII.[79] This privacy policy was changed in 2011 to permit the sale of personal information in the sale or reorganization of Quirky's business.[80] Quirky maintained that a consumer privacy ombudsman was not required because its post-2011 privacy policy, *i.e.*, the privacy policy on the petition date, permitted the sale of PII.[81] The U.S. Trustee countered that Quirky's prior privacy policy continued to have application to the PII of customers who had not consented to the revised privacy

---

[74] *See id.* at 19–20 (describing a policy, which required consumer consent to disclose information to third parties).

[75] *Id.* at 19.

[76] *See id.* at 31–34 ("Prior to May 28, 2008, a reasonably prudent consumer would not have expected a sale of his or her PII, and, if apprised of the existence of a 'sale' provision, might not have provided PII to Debtor.").

[77] *See* Order Approving Sale, *supra* note 70, at *49–50 (specifying the terms negotiated that allowed the sale of PII).

[78] *See* Debtors' Mot. for Entry, *supra* note 54, at 3, 37–38 (detailing the assets that the debtor sought to sell).

[79] *See* Objection to Debtor's Mot., *supra* note 20, at 2–3.

[80] *See id.* at 5 (explaining before 2011 Quirky's privacy policy did not permit the sale of PII).

[81] *See* Debtor's Mot. for Entry, *supra* note 54, at 21 ("Accordingly, the Debtors believe that the sale of the Quirky Assets, including any personally identifiable information, complies with the Quirky privacy policy, is appropriate and should be approved, and that the appointment of a consumer privacy ombudsman is not necessary.").

policy.[82] According to the U.S. Trustee, many customers who had agreed to the earlier privacy policy had not visited Quirky's website since the change in policy, and Quirky's terms of service did not provide that the privacy policy could change without notice to customers.[83] Consequently, the sale of those customers' personal information was inconsistent with the privacy policy they had agreed to, and required the appointment of a consumer privacy ombudsman.[84] The matter was settled by the debtor agreeing with the U.S. Trustee to exclude the PII of customers who did not log in to the Quirky website at any time after the less restrictive privacy policy was adopted.[85]

Quirky is a particularly interesting case for several reasons. First, the existence of Quirky's prior privacy policy that prohibited the sale of PII was referenced only vaguely in its motion.[86] Debtors do not always disclose the existence of a prior privacy policy. Perhaps because they believe—like Quirky—that the privacy policy on the petition date is the only privacy policy that matters. Quirky's disclosure consisted of a vague reference in a footnote, which required a reader of considerable diligence and skill to discover the existence of the prior privacy policy that prohibited the sale of PII.[87] Second, the U.S. Trustee identified the issue when others may have overlooked it or had little incentive to pursue it.[88] Finally, in the absence of the appointment of a consumer privacy ombudsman, the privacy interests of Quirky's customers were protected by the U.S. Trustee. As a practical

---

[82] *See* Obj. to Debtors' Mot., *supra* note 20, at 5 ("While the privacy policy that was effective as of March 2011 provided for its terms of service to be changed without any additional notice, for those Quirky community members who joined prior to March 2011, their terms of service would only be changed if they logged on to the Quirky website after March 2011.").

[83] *See id.* ("The Debtors do not provide any information with respect to how many of Quirky community members that were on or prior to March 2011 and how many of these members logged into the Quirky Website on or after March 2011.").

[84] *See id.* at 2.

[85] *See* Certification of Counsel Regarding Order (I) Approving Bidding Procedures and Bid Protections in Connection with the Sale of Certain Assets Related to the Business of Quirky, Inc., (II) Approving Procedures for Assumption and Assignment of Executory Contracts, (III) Approving the Form and Manner of Notice, and (IV) Scheduling an Auction and a Sale Hearing at 2, *In re* Quirky, Inc., No. 15-12596 (Bankr. S.D.N.Y. Oct. 27, 2015) [hereinafter Certification of Counsel] (indicating the debtors and U.S. Trustee were in negotiations); *see also* Order (I) Approving Bidding Procedures and Bid Protections in Connection with the Sale of Certain Assets Related to the Business of Quirky, Inc., (II) Approving Procedures for Assumption and Assignment of Executory Contracts, (III) Approving the Form and Manner of Notice, and (IV) Scheduling an Auction and a Sale Hearing at 9, *In re* Quirky, Inc., No. 15-12596 (Bankr. S.D.N.Y. Oct. 27, 2015) ("Notwithstanding anything in the Quirky Sale Motion or the Quirky Bidding Procedures to the contrary, the sale of Quirky assets shall not include the Personally Identifiable Information of those members of the Quirky Community and Platform that did not log in at any time on or after October 2011.").

[86] *See* Debtors' Mot. for Entry, *supra* note 54, at 21 n.5 (mentioning the prior privacy policy in a footnote).

[87] *See id.* at 21 n.6 ("The Quirky terms of service provides that Quirky reserves 'the right, at [its] sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice.' Any change to the terms of service requires a Quirky user to accept the changes upon the first login after the changes to the terms of service were made. *To the extent any Quirky users exist that pre-date the adoption of the above referenced acceptable use of personally identifiable information (March 2010), any such users became bound by the above language by their further use of the Quirky website.*") (emphasis added) (internal citations omitted).

[88] *See generally* Obj. to Debtor's Mot., *supra* note 20.

matter, it will often fall to the U.S. Trustee to ensure that the privacy interests of consumers are protected when PII is sold in bankruptcy.

CONCLUSION

A debtor's PII may be subject to multiple privacy policies; not necessarily only the debtor's privacy policy on the petition date. The goal of protecting consumer privacy is better served by subjecting the personal information of consumers to the privacy policy to which they consented, rather than to subsequent privacy policies of which they may not even be aware. As one commentator observed:

> The sale of sensitive PII to the highest bidder in a bankruptcy sale, as envisioned by many recently published company privacy policies, without oversight of the bankruptcy court, a consumer privacy ombudsman, or entity charged with enforcing consumer protection laws, means that any person or entity, anywhere in the world, in any line of business, and for whatever reason, could purchase the biometric identifiers, geolocation data, healthcare records, private data recorded in a connected vehicle, and children's information, of many millions of individuals.[89]

The requirement for the appointment of a consumer privacy ombudsman turns on whether the privacy policy "in effect on the date of the commencement of the case" prohibits the transfer of PII.[90] This refers to the privacy policy that applies to the particular PII in question, not necessarily the privacy policy in place on the petition date. As a result, a debtor's database of PII may be governed by more than one privacy policy. This is consistent with both the statutory text of the Bankruptcy Code and longstanding FTC principles regarding consumer consent to material retroactive changes to privacy practices.

The sale of PII creates tension between maximizing the value of the debtors' assets and protecting the privacy interests of consumers. Moreover, because of the administrative costs to the bankruptcy estate of a consumer privacy ombudsman, debtors and creditors may not view the ombudsman's appointment to be in their interests and may have little incentive to favor such an appointment. As a result, unless it is a high-profile case that has attracted the attention of the FTC or states' attorneys general, it will often fall to the U.S. Trustee to ensure that consumers' privacy interests are protected in bankruptcy sales of PII.

---

[89] Lucy L. Thomson, *Sensitive Personal Data for Sale in Bankruptcy—An Uncertain Future for Privacy Protection*, NORTON ANN. SURV. OF BANKR. L. 343, 358–59 (2017).

[90] *See* 11 U.S.C. § 363(b)(1) (2012).