Emory Bankruptcy Developments Journal

Volume 33
Issue 2 *The Fourteenth Annual Emory Bankruptcy Developments Journal Symposium*

Article 5

2017

Coming to a Retailer Near You: Consumer Privacy Protection in Retail Bankruptcies

Kayla Siam

COMING TO A RETAILER NEAR YOU: CONSUMER PRIVACY PROTECTION IN RETAIL BANKRUPTCIES

ABSTRACT

Consumers' personally identifiable information is an extremely valuable asset for retailers. As a result, retailers often sell such consumer information to pay creditors in bankruptcy. The sale of consumer information causes problems for consumers because many retailers transfer personally identifiable information to third parties without notifying consumers beforehand and without obtaining their consent. Perhaps most troubling, however, is that retailers facing financial turmoil sometimes sell personally identifiable information in direct violation of their own privacy policies, which specifically promise the safeguarding of consumer information. The Federal Trade Commission, State Attorneys General, independent consumer privacy agencies, and some retailers have objected to such transfers, but to no avail.

Because of inconsistent consumer privacy enforcement, loose protections of consumer information within the Bankruptcy Code, and an imbalance between the principles of debtor rehabilitation and consumer privacy, courts have permitted retailers to sell personally identifiable information in bankruptcy even when such sales violate retailers' privacy policies. This Comment addresses the shortcomings of current privacy regulations both inside and outside of bankruptcy law. Additionally, this Comment recommends the implementation of minimum federal privacy standards and suggests that the Bankruptcy Code include stronger consumer privacy guidelines. These approaches would allow consumers to have a say in who receives their personally identifiable information while simultaneously preserving both the current privacy regulation infrastructure and a retailer's ability to attain rehabilitation in bankruptcy.

INTRODUCTION

Over the past decade, many retailers have filed for bankruptcy relief in the United States.[1] These bankruptcy filings pose risks for consumers because the debtors can sell consumers' personally identifiable information ("PII") to repay their debts.[2] In 2015, RadioShack, an electronics retailer, intended to sell PII through an asset sale during its bankruptcy proceedings.[3] Government authorities, consumer advocates, and other retailers, however, objected to the initial sale attempt.[4] The Federal Trade Commission ("FTC") intervened in the proceedings through its ability to prosecute unfair and deceptive practices affecting commerce.[5] The Attorney General of Texas, with support from Attorneys General of many other states, objected to the sale to protect the consumer privacy rights of its residents.[6] Other large retailers also objected to the sale to protect consumer information previously shared with the retail debtor.[7]

The filings in RadioShack's bankruptcy case stirred debate among practitioners concerning how retail bankruptcy cases should handle the sale of

---

[1] *See Business Bankruptcy Filings - 2005–2015*, AM. BANKR. INST., http://www.abi.org/node/234505 (last visited Jan. 20, 2016).

[2] *See generally* Debtors' Consolidated Reply in Supp. of IP Sale, *In re* RadioShack Corp., No. 15-10197 (Bankr. D. Del. May 19, 2015), 2015 WL 3380982; State of Tex. Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *In re* RadioShack Corp., No. 15-10197 (Bankr. D. Del. Mar. 20, 2015), 2015 WL 2375420; Joshua Brustein, *RadioShack's Bankruptcy Could Give Your Customer Data to the Highest Bidder*, BLOOMBERG BUS. (Mar. 24, 2015, 10:03 AM), http://www.bloomberg.com/news/articles/2015-03-24/RadioShack-s-bankruptcy-could-give-your-customer-data-to-the-highest-bidder; Chris Isidore, *RadioShack Sale Protects Most Customer Data*, CNNMONEY (June 10, 2015, 4:16 PM), http://money.cnn.com/2015/06/10/news/companies/RadioShack-customer-data-sale/.

[3] *See* Debtors' Consolidated Reply in Supp. of IP Sale, *supra* note 2, ¶ 1.

[4] *See* Allison Grande, *FTC Wades Into Fight Over RadioShack's Customer Data Sale*, LAW360 (May 18, 2015, 9:53 PM), http://www.law360.com/articles/657039/ftc-wades-into-fight-over-RadioShack-s-customer-data-sale; Isidore, *supra* note 2; Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.* 3, (May 16, 2015), https://www.ftc.gov/system/files/documents/public_statements/643291/150518radioshackletter.pdf.

[5] *See* Press Release, Federal Trade Commission, FTC Requests Bankruptcy Court Take Steps to Protect RadioShack Consumers' Personal Information (May 18, 2015), https://www.ftc.gov/news-events/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-RadioShack; Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4; *see also* 15 U.S.C. § 45(a) (2012).

[6] *See* State of Tex. Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2, ¶ 11; Suppl. to Ltd. Obj. Filed by the State of Tex. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, ¶¶ 2, 3, *In re* RadioShack Corp., No. 15-10197 (Bankr. D. Del. 2015); Brustein, *supra* note 2; Isidore, *supra* note 2.

[7] *See* Debtors' Consolidated Reply in Supp. of IP Sale, *supra* note 2, ¶¶ 4, 10–13; Brustein, *supra* note 2; Grande, *supra* note 4.

consumer information.[8] On the one hand, consumer information can be an extremely valuable asset for a retailer to use to repay creditors.[9] On the other hand, sharing PII without receiving consent from the consumer could potentially violate consumer privacy,[10] increase the risk of fraud and identity theft,[11] and impair the control other businesses have over their consumer information.[12] Currently, federal law does not require companies to have privacy policies.[13] Additionally, if a company chooses to establish a privacy policy, it is not required to inform consumers about how it will use their PII.[14] Additionally, the Bankruptcy Code (the "Code") does not directly protect consumer privacy when retailers sell consumer information in bankruptcy.[15]

Because the federal government does not articulate general consumer privacy expectations, there are gaps in the current state and sector-specific

---

[8] *See generally* Jack Butler, *The Examiners: Consumers Face Pain and Opportunity in Bankruptcy*, WALL ST. J. BANKR. BEAT (July 30, 2015, 12:31 PM), http://blogs.wsj.com/bankruptcy/2015/07/30/the-examiners-consumers-face-pain-and-opportunity-in-bankruptcy/; Lisa Donahue, *The Examiners: Buyer Beware*, WALL STREET J. BANKR. BEAT (July 30, 2015, 11:43 AM), http://blogs.wsj.com/bankruptcy/2015/07/30/the-examiners-buyer-beware/; Jay Goffman, *The Examiners: Balance Shoppers' Privacy With Need to Maximize Value*, WALL STREET J. BANKR. BEAT (July 30, 2015, 10:34 AM), http://blogs.wsj.com/bankruptcy/2015/07/30/the-examiners-balance-shoppers-privacy-with-need-to-maximize-value/; Shaunna D. Jones, *The Examiners: Don't Disrupt Bankruptcy's Level Playing Field*, WALL STREET J. BANKR. BEAT (July 29, 2015, 1:52 PM), http://blogs.wsj.com/bankruptcy/2015/07/29/the-examiners-dont-disrupt-bankruptcys-level-playing-field/; Sharon Levine, *The Examiners: Existing Safeguards Protect Shoppers*, WALL STREET J. BANKR. BEAT (July 29, 2015, 11:26 AM), http://blogs.wsj.com/bankruptcy/2015/07/29/the-examiners-existing-safeguards-protect-shoppers/; Mark Roe, *The Examiners: Assure Consumers That Gift Cards, Privacy Will be Protected*, WALL STREET J. BANKR. BEAT (July 28, 2015, 11:17 AM), http://blogs.wsj.com/bankruptcy/2015/07/28/the-examiners-assure-consumers-that-gift-cards-privacy-will-be-protected/.

[9] *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, 834 (2001); Carl Steidtmann, *Column, Turnaround Topics, The Impact of E-retailing*, 19-3 AM. BANKR. INST. J., 24 (2000); *see also* Press Release, Federal Trade Commission, FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations (July 21, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding; Brustein, *supra* note 2; Grande, *supra* note 4.

[10] *See* 15 U.S.C. § 45(a).

[11] *See* Lucy L. Thomson, *Personal Data for Sale in Bankruptcy: A Retrospective on the Consumer Privacy Ombudsman*, 34-6 AM. BANKR. INST. J. 32, 32 (2015).

[12] *See* Debtors' Consolidated Reply in Supp. of IP Sale, *supra* note 2, ¶¶ 4, 10, 13; Brustein, *supra* note 2; Grande, *supra* note 4.

[13] *See generally Privacy Law*, U.S. SMALL BUS. ASS'N., https://www.sba.gov/content/privacy-law (last visited Oct. 28, 2015).

[14] *See generally id*.

[15] *See* Miller, Jr. & O'Rourke, *supra* note 9, at 817; Jenn Topper et al., *Consumer Data In Bankruptcy: Saleable Asset Or Liability?*, LAW360 (Apr. 10, 2015, 10:23 AM), https://www.law360.com/articles/641433/consumer-data-in-bankruptcy-saleable-asset-or-liability- ("The Bankruptcy Code does not call for comprehensive protections of data or guidelines as to its use with respect to a sale or liquidation.").

protections.[16] This Comment discusses the need for explicit federal regulations that create minimum privacy standards for businesses to comply with to avoid inconsistent consumer privacy protections and enforcement by the states. Specifically, this Comment suggests that Congress require all businesses collecting consumer information to establish privacy policies. Further, the Code should specifically address adherence to privacy policies to protect PII subject to transfer in asset liquidations. The combination of these protections would provide stronger federal safeguards for consumers when retailers file for bankruptcy and properly balance consumer interests with the implicit policies of bankruptcy law.

Part I.A of this Comment discusses the few Code provisions that marginally relate to the sale of consumer information in bankruptcy proceedings. Part I.B examines the outcomes of two illustrative cases involving the sale of consumer information, which have developed many of the standards for consumer information asset sales in retail bankruptcies. Part II.A analyzes how and why retailers collect consumer information and how these collection efforts affect consumer privacy. Part II.B then analyzes current methods used to prevent the improper sale of consumer information in bankruptcy and the limitations of these methods. Part II.C considers many of the proposals suggested by legislators, judges, commissioners of the FTC, and other legal practitioners to strengthen the privacy protections of consumers in retail bankruptcies. Finally, This Comment concludes that the implementation of minimum privacy standards for businesses through federal legislation and the Code is crucial to adequately protect consumers from retailers selling their PII in bankruptcy. These measures would protect the privacy rights of the retail debtor's past customers while also allowing the retail debtor to have an opportunity to appropriately gain value from a delicate asset.

I. BACKGROUND

In 2005, nearly 40,000 businesses filed for bankruptcy relief in the United States.[17] This figure reached 60,000 in 2009.[18] Although the volume of business filings has steadily decreased since 2009, between 2005 and 2015, there have been over 400,000 business bankruptcy filings.[19] Many speculators

---

[16] *See generally* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 872–73 (2009).

[17] *See Business Bankruptcy Filings*, *supra* note 1.

[18] *See id*.

[19] *See id*.

have attributed the large number of business bankruptcies over this decade to the economic recession that began in 2006, the turmoil and instability of credit and equity markets,[20] the real estate burdens across numerous industries, depressed consumer spending, and shifts in consumer shopping habits.[21] Companies, both large and small, commonly are involved in liquidations, buyouts, and reorganizations while in bankruptcy.[22] Some of these processes make consumer information gathered by retail debtors during its business operations more vulnerable.[23] Unpermitted access to consumer information through asset sales can implicate a variety of legal issues relating to regulatory matters and, more specifically, consumer protection laws.[24] Many courts have wrestled with trying to protect consumer privacy in cases where retail businesses wish to sell their consumer information through asset liquidations.[25]

The three common assets that retailers tend to sell in asset liquidations are inventory, real estate, and intangible intellectual property.[26] While tangible assets tend to deflate in value over time, intangible assets, such as consumer information, tend to increase in value—making consumer information a critical asset for a retail debtor seeking to survive bankruptcy.[27] The sale of consumer information, however valuable, can become a significant liability if the consumer's information is used improperly, gets into the wrong hands, or violates privacy protections.[28]

Though the Code does not directly address consumer privacy, some provisions offer limited guidance regarding the sale of confidential information

---

[20] *See* Neil E. Harmon, *Chapter 11 Cases Involving Retail Businesses*, *in* COLLIER GUIDE TO CHAPTER 11: KEY TOPICS AND SELECTED INDUSTRIES ¶ 20.01 (Alan N. Resnick & Henry J. Sommer eds. 2014).

[21] *See* Anders J. Maxwell, *The Examiners: Retail Distress of More Concern Than Consumers,* WALL STREET J. BANKR. BEAT (July 28, 2015, 11:59 PM), http://blogs.wsj.com/bankruptcy/2015/07/28/the-examiners-retail-distress-of-more-concern-than-consumers/.

[22] Topper et al., *supra* note 15.

[23] *See* Thomson, *supra* note 11; Topper et al., *supra* note 15 ("Data leakage, in industry terms, is a severe and growing problem especially in instances such as a bankruptcy filing of a retailer or any company retaining customer records and personally identifiable information or financial details.").

[24] *See* Harmon, *supra* note 20, ¶ 20.04.

[25] *See generally* State of Tex. Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2; *In re* JK Harris & Co., LLC, 475 B.R. 470 (Bankr. D.S.C. 2012); *In re* Borders Grp., Inc., No. 11-10614 MG, 2011 WL 5520261 (Bankr. S.D.N.Y. 2011); *In re* ZTBK, INC., f/k/a Zestra Laboratories, Inc., No. 108BK11313, 2009 WL 4906708 (Bankr. D. Del. 2009); F.T.C. v. Toysmart.com, Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. 2000).

[26] *See* Harmon, *supra* note 20, ¶ 20.07.

[27] *See* Steidtmann, *supra* note 9.

[28] *See* Thomson, *supra* note 11; Topper et al., *supra* note 15 ("Patching the holes in easily identifiable scenarios such as bankruptcy is a surmountable solution that can end a massive data breach that has a ripple effect across payment processors, banks, insurers, retailers and software providers.").

in general.[29] The pivotal cases concerning the liquidation of consumer information illustrate how bankruptcy courts apply both bankruptcy and nonbankruptcy law when retail debtors attempt to sell consumer information in direct violation of their privacy policies.[30] This section provides a brief overview of the applicable Code provisions that guide the sale of information and the case law that demonstrates how bankruptcy courts have handled consumer information asset sales.

A. Statutory Background: The Code

The two main principles underlying bankruptcy law are the rehabilitation of the "honest but unfortunate debtor"[31] and the equitable treatment of the debtor's creditors.[32] For businesses, rehabilitation may include business reconstruction, known as reorganization, to prevent the loss of jobs and misuse of resources that could ensue if the debtor went out of business.[33] Inherent in reorganization is the goal of value-maximization to reach optimal levels of distribution to the business's creditors.[34] The Code sets out the provisions that govern bankruptcy law in a manner consistent with these principles.[35]

In 2005, Congress passed the Bankruptcy Abuse Prevention and Consumer Protection Act ("BAPCPA"), which added provisions to the Code affecting consumer privacy.[36] After BAPCPA's enactment, §§ 107, 332, and 363 of the Code had limited impact upon the sale of consumer information in retail bankruptcies.[37] Together, these provisions provide for the confidentiality of certain types of information,[38] the sale of PII,[39] and the appointment of a

---

[29] *See generally* 11 U.S.C. §§ 107(b), 332, 363(b) (2012).

[30] *See generally Toysmart.com*, 2000 WL 1523287; *In re* RadioShack Corp., No. 15-10197 (Bankr. D. Del. 2015).

[31] 1 COLLIER ON BANKRUPTCY ¶ 1.01 (Alan N. Resnick & Henry J. Sommer eds., 16th ed.) (quoting Marrama v. Citizens Bank of Mass., 549 U.S. 365, 367 (2007)).

[32] *See* 1 COLLIER, *supra* note 31, ¶ 1.01.

[33] *See id.* (citing NLRB v. Bildisco & Bildisco, 465 U.S. 513, 528 (1984) and United States v. Whiting Pools, Inc., 462 U.S. 198, 203 (1983)).

[34] *See* 1 COLLIER, *supra* note 31, ¶ 15.01.

[35] *See id*, ¶ 1.01.

[36] *See* Bankruptcy Abuse Prevention and Consumer Protection Act of 2005, Pub. L. No. 109-8, 119 Stat. 23 (2005); Thomson, *supra* note 11.

[37] *See* Thomson, *supra* note 11; *see also* 11 U.S.C. §§ 107(b), 332, 363(b) (2012).

[38] *See* 11 U.S.C. § 107(b).

[39] *Id.* § 363(b). *See generally* State of Tex.'s Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2; Kenneth M. Misken & Camisha L. Simmons, *Government Addresses Privacy Concerns in Bankruptcy Sales*, 31-10 AM. BANKR. INST. J. 28, 28 (2012);

consumer privacy ombudsman in bankruptcy proceedings where the debtor proposes to sell PII.[40]

Under § 107 of the Code, a court may, and sometimes must, protect an entity's trade secrets, confidential research, development, or commercial information.[41] Many states define a "trade secret" as information that derives independent economic value by remaining secret where the debtor has taken reasonable measures to maintain the secrecy of the information.[42] Section 107 further states that a court may protect an individual, with respect to any information filed with the court, "to the extent the court finds that disclosure of such information would create undue risk of identity theft or other unlawful injury to the individual or the individual's property."[43] Although this provision could adequately protect consumer information when a retail debtor does not wish to use or reveal it during the bankruptcy process, this provision does not protect consumer information when the retail debtor intends to release or sell consumer information it has gathered.[44]

Section 363 essentially mandates that a debtor may not sell or lease PII where a policy was in effect on the petition date unless: (1) the transfer is consistent with the policy; or (2) the court approves the sale after the appointment of a consumer privacy ombudsman and notice and a hearing.[45] The Code defines PII as an individual's first and last name, email address, phone number, social security number, credit card information, possibly birth date, or any other information that can be used to contact or identify the individual.[46] Section 363 requires the appointment of a consumer privacy ombudsman in bankruptcy cases where the debtor considers selling PII in a manner that the court believes is inconsistent with the debtor's existing privacy policy at the time of filing.[47] If a consumer privacy ombudsman is appointed, the court may approve the sale only after "(i) giving due consideration to the

---

Thomson, *supra* note 11; Topper et al., *supra* note 15; Committee Educational Session: Asset Sales/Technology and Intellectual Property, 120111 ABI-CLE 433 (2011).

40 *See* 11 U.S.C. § 332.

41 *See id.* § 107(b).

42 *See generally* CAL. CIV. CODE § 3426.1 (West 2013); DEL. CODE ANN. tit. 6, § 2001 (West 2014); FLA. STAT. ANN. § 688.002 (West 2014); 765 ILL. COMP. STAT. ANN. 1065/2 (West 2012); MINN. STAT. § 325C.01 (West 2015); 12 PA. STAT. AND CONS. STAT. ANN. § 5302 (West 2014); WASH. REV. CODE ANN. §19.108.010 (West 2012).

43 11 U.S.C. § 107(c).

44 *See id.*

45 *See id.* § 363(b)(1).

46 *See id.* § 101(41A).

47 *See id.* § 363(b)(1); *see also* Thomson, *supra* note 11.

facts, circumstances, and conditions of such sale . . . and (ii) finding that no showing was made that such sale . . . would violate applicable nonbankruptcy law."[48]

Section 332 of the Code specifically addresses the appointment and duties of a consumer privacy ombudsman.[49] Section 332 requires the appointment of a disinterested person to serve as a consumer privacy ombudsman if a hearing is required under § 363(b)(1)(B) (a sale of PII outside the ordinary course of business and in violation of the debtor's current privacy policy).[50] A consumer privacy ombudsman is authorized to "investigate and provide the court with information relating to the debtor's privacy policy, potential losses or gains of privacy and potential costs or benefits to customers if the sale is approved, and possible alternatives that would mitigate potential privacy losses or costs to consumers."[51]

Sections 107, 332, and 363 of the Code offer limited protections of consumer information in bankruptcy cases. Although these provisions set some standards on the sale of PII, these protections are limited in practice, such as when a retail debtor affirmatively chooses to transfer collected consumer information, regardless of whether the transfer complies with the debtor's privacy policy. The following case law interpretations of the provisions demonstrate how the Code's protections of PII effectively take shape.

B. Case Law Background: Then and Now

A mere reading of the Code provisions that apply to the sale of PII may not offer enough insight into how these rules are applied in bankruptcy cases. To better understand how a bankruptcy court handles the sale of consumer information, this section compares the seminal case that created the initial standards for the transfer of PII to a recent case that involved a substantially similar transfer.[52] The result of one of the most recent cases involving the sale of consumer information in a retail bankruptcy has stirred debate on the

---

[48] 11 U.S.C. § 363(b)(1).

[49] *See id.* § 332(a).

[50] *See id*.

[51] Thomson, *supra* note 11; *see* 11 U.S.C. § 332(b) (delineating consumer privacy ombudsman's role in "assist[ing] the court in its consideration of the facts, circumstances, and conditions of the proposed sale . . . of" PII).

[52] *See* F.T.C. v. Toysmart.com, Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. 2000); *In re* RadioShack Corp., No. 15-10197 (Bankr. D. Del. 2015).

implementation and effectiveness of consumer privacy outcomes in bankruptcy courts.[53]

1. The Beginning: F.T.C. v. Toysmart.com

The FTC first set the standards for the sale of consumer information in bankruptcy proceedings in *F.T.C. v. Toysmart.com*.[54] Toysmart.com was an online retailer of educational toys for children.[55] Toysmart.com collected PII "including, but not limited to, consumers' names, addresses, billing information, shopping preferences, and family profile information," and then attempted to sell the consumer information after filing for bankruptcy in June 2000.[56] The retailer, however, had assured its customers that their "information w[ould] never be shared with a third party."[57] Specifically, Toysmart.com's privacy policy stated, "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. All information obtained by toysmart.com is used only to personalize your experience online."[58]

The FTC filed a complaint with the bankruptcy court[59] objecting to Toysmart.com's attempt to sell PII because such a sale would violate the company's privacy policy and therefore could potentially violate § 5(a) of the Federal Trade Commission Act ("FTCA") as a deceptive practice.[60] Toysmart.com and the FTC reached an agreement where the debtor consented to strict standards for the sale of the consumer information.[61] The agreement stipulated that: (1) PII could not be sold as a standalone asset; (2) the buyer of the information must be engaged in substantially the same line of business as the seller; (3) the buyer must expressly agree to be bound by and adhere to the seller's privacy policy with respect to personal information acquired from the seller; and (4) the buyer must obtain affirmative consent from customers for

---

[53] *See generally* Butler, *supra* note 8; Donahue, *supra* note 8; Goffman, *supra* note 8; Jones, *supra* note 8; Levine, *supra* note 8; Roe, *supra* note 8.

[54] *See* Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

[55] *See* Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9.

[56] *See* Complaint, F.T.C. v. Toysmart.com, No. 00-11341-RGS, 2000 WL 34575570 (D. Mass. 2000); *see also Toysmart.com*, 2000 WL 1523287.

[57] Complaint, Toysmart.com, 2000 WL 34575570.

[58] *Id*.

[59] *See id*.

[60] *See* Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

[61] *Id*.

any material changes that may affect the information collected under the seller's privacy policy.[62] The FTC reasoned that if the purchaser abided by these conditions, then the purchaser would not be considered a "third party" under the privacy policy but, rather, a "qualified buyer,"[63] thus alleviating any contradiction to the seller's privacy policy.[64]

Even though Toysmart.com and the FTC reached an agreement, the FTC narrowly approved the settlement's terms and restrictions, with two commissioners dissenting.[65] Commissioner Sheila F. Anthony stated that she disapproved of the settlement because it placed "business concerns ahead of consumer privacy."[66] Commissioner Orson Swindle stated that he believed the settlement allowed businesses to break the "promises they make to consumers"; specifically, the promise that the company "would *never* be sold to a third party."[67] Although Commissioner Mozelle W. Thompson voted in favor of the settlement, he stated that the company's lack of success should not extinguish its obligations to its customers and that his "decision to approve the settlement [was] not without reservation."[68]

Others agreed with the concerned commissioners' views regarding the potential harm that could be caused even if the purchasers were deemed "qualified buyers."[69] Many parties objected to the transfer of PII, including State Attorneys General and independent data privacy companies.[70] Additionally, Judge Carol Kenner, the bankruptcy judge presiding over the case, said that she had "fundamental problems" with the settlement and would likely support the state's objections to the transfer.[71] Ultimately, Toysmart.com withdrew from the sale entirely, relieving the court from determining whether

---

62 *See id*.

63 The FTC argued for a legal fiction: a "qualified buyer" was not the same as a "third party" because the former was "a company that concentrates its business in the same industry as a debtor, intends to purchase a debtor's goodwill, agrees to become a debtor's successor-in-interest as to the customer information, and agrees to abide by the terms of a debtor's privacy policy." 17-CM COLLIER ON BANKRUPTCY, *supra* note 31, ¶ 30.02.

64 *See id*.

65 *See* Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9.

66 *Id*.

67 *Id.*; *see also* 17-CM COLLIER ON BANKRUPTCY, *supra* note 31, ¶ 30.02.

68 Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9.

69 *See* 17-CM COLLIER ON BANKRUPTCY, *supra* note 31, ¶ 30 ("Forty-six states, the District of Columbia, and two territories agreed with Commissioner Swindle's position and filed an objection with the bankruptcy court to the FTC's stipulated settlement based upon state privacy laws.").

70 *See* Miller, Jr. & O'Rourke, *supra* note 9, at 794.

71 *See* Stephanie Stoughton, *Judge Disputes FTC Settlement on Web Store Database*, BOS. GLOBE, Jul. 27, 2000, at E5; Miller, Jr. & O'Rourke, *supra* note 9, at 794.

to approve or deny the transfer.[72] Nevertheless, the conditions set forth by the FTC in the initial settlement set the standard that future bankruptcy courts would follow in retail bankruptcies involving the sale of consumers' PII.[73]

2. Modern Day: In re RadioShack Corp.

In February 2015, RadioShack, an electronics retailer, filed for chapter 11 bankruptcy.[74] Many sources claimed that RadioShack had access to the PII of over 117 million consumers,[75] which accounted for approximately 37% of the United States' population in 2015.[76] RadioShack had collected the names, addresses, email addresses, payment card numbers, purchase history, and other personal information of its customers.[77] RadioShack's privacy policy stated that it would neither sell its mailing list nor sell or rent any consumer information "to anyone at anytime."[78]

Following RadioShack's bankruptcy filing, the ninety-four-year-old company offered to auction off its trademarks, patents, leases, and consumer information.[79] Texas Attorney General Ken Paxton filed an objection, supported by twenty-one governmental consumer protection entities,[80] arguing that the sale was impermissible under § 363(b)(1)(B)(ii)[81] because it violated the Texas Deceptive Trade Practices Act's prohibition of "[f]alse, misleading,

---

72 *See* Miller, Jr. & O'Rourke, *supra* note 9, at 794.

73 *See* Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

74 Prelim. Obj. & Reservation of Rights of Cellco P'ship d/b/a Verizon Wireless to Debtors' Mot. for Entry of Interim and Final Orders, *In re* RadioShack Corp., No. 15-10197, 2015 WL 757150 (Bankr. D. Del. 2015); Grande, *supra* note 4.

75 State of Tex.'s Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2; Isidore, *supra* note 2; Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

76 State of Tex.'s Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2, at n.2.

77 *See id.* ¶ 3; Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

78 State of Tex.'s Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2; Grande, *supra* note 4; *see* Brustein, *supra* note 2.

79 *See* Brustein, *supra* note 2.

80 Suppl. to Ltd. Obj. Filed by the State of Tex. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 6.

81 *See* State of Tex.'s Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note2; *see also* 11 U.S.C. § 363(b)(1)(B)(ii) (2012).

or deceptive practices." [82] The sale amounted to a deceptive act in clear violation of Texas law because, according to its terms, RadioShack would dishonor its own privacy policy.[83]

Past business affiliates of RadioShack, such as AT&T, Verizon, and Apple, also joined in objecting to the sale of consumer information to protect their customers' PII, which RadioShack had received in prior business transactions.[84] RadioShack collected the PII of customers regardless of what product or service plan the customers purchased.[85] A number of the products and services RadioShack offered to customers were provided by RadioShack affiliates and other external retailers.[86] Many of these external retailers claimed to have clauses within their contract agreements with RadioShack that prohibited the sale of consumer information derived from customers who purchased their products and services.[87] RadioShack affiliates argued that RadioShack had no right to the consumer information collected from the affiliates' customers because "the information [was not] RadioShack's to sell."[88] Some affiliates believed that the asset sale could potentially cause the transfer of their customer information to competing companies.[89] As a result, many affiliates demanded the destruction of consumer information gathered through their product and service sales.[90]

RadioShack argued that customers who purchased products and services from external retailers in their stores were actually shared customers, not the sole customers of its affiliates.[91] In fact, RadioShack maintained that shared customers were "first and foremost, a RadioShack customer," regardless of what company created the product or service purchased.[92] To alleviate the concerns the affiliates expressed, RadioShack removed all information that

---

[82] State of Tex.'s Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2 (quoting TEX. BUS. & COM. CODE § 17.46 (West 2014)).

[83] *See* State of Tex.'s Ltd. Obj. to Sale of Personally Identifiable Info. of One Hundred Seventeen Million Consumers, *supra* note 2, ¶¶ 11–17.

[84] *See* Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, ¶¶ 4, 11. *See generally* Brustein, *supra* note 2; Grande, *supra* note 4; Isidore, *supra* note 2.

[85] *See* Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, ¶ 11.

[86] *See id.* ¶ 12.

[87] *See id.* ¶ 13.

[88] Brustein, *supra* note 2; *see* Grande, *supra* note 4.

[89] *See* Brustein, *supra* note 2; *see also* Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, ¶ 19.

[90] *See* Brustein, *supra* note 2.

[91] *See* Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, ¶ 15.

[92] *Id.* ¶ 11.

related to or referenced affiliate retailers before the sale of any consumer information.[93] The court ultimately approved the transfer.[94]

The court appointed a consumer privacy ombudsman because the case involved the sale of consumer information that could potentially violate the retail debtor's privacy policy.[95] In a letter to the consumer privacy ombudsman, the Director of the FTC's Office of the Bureau of Consumer Protection offered two alternatives: RadioShack would have to either (1) receive affirmative consent from their customers to transfer their PII; or (2) abide by specific conditions to sell the consumer information.[96] Similar to the conditions relayed in the *Toysmart.com* settlement, the FTC requested the following conditions be imposed on the sale: (1) the customer information could not be sold as a standalone asset; (2) the buyer had to be engaged in substantially the same lines of business as RadioShack; (3) the buyer had to expressly agree to be bound by and adhere to the terms of RadioShack's privacy policy that pertained to the personal information acquired from RadioShack; and (4) the buyer had to agree to obtain affirmative consent from consumers for any material changes to the privacy policy.[97] The FTC's repeated use of these conditions essentially formed the standard courts should use in future bankruptcies where retailers wish to sell consumer information.[98]

RadioShack sold its consumer information for $26.2 million[99] to General Wireless Operations, Inc., one of RadioShack's majority shareholders.[100] At the time of sale, General Wireless intended to keep about 1,700 stores operational under the RadioShack name after the bankruptcy concluded.[101] RadioShack and General Wireless made an agreement with over thirty State Attorneys General regarding what information could be transferred in the

---

[93] *See id.* ¶¶ 9, 14–15.

[94] *See* Peg Brickley, *Standard General Gets Nod to Buy RadioShack Data*, DOW JONES DAILY BANKR. REV. (May 20, 2015, 10:48 PM), http://www.newsjs.com/url.php?p=http://bankruptcynews.dowjones.com/Article?an=DJFDBR0120150520eb5knu2zi&cid=32135012&ctype=ts&pid=310.

[95] *See* Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4; *see also* Brustein, *supra* note 2.

[96] *See* Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

[97] *Id.*

[98] *See id*.

[99] The final purchase price was more than double the initial bid ask price of $12 million. Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, at ¶ 1.

[100] *Id.* ¶ 1; *see* Grande, *supra* note 4; Isidore, *supra* note 2.

[101] Grande, *supra* note 4; Isidore, *supra* note 2; *see* Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, ¶¶ 3, 19; Peg Brickley, *supra* note 95.

sale.[102] From the names, addresses, email addresses, payment card numbers, purchase history, and other customer information collected, RadioShack and General Wireless guaranteed that consumer financial information, social security numbers, dates of birth, and phone numbers would not be sold in the asset transfer.[103] After the purchase, General Wireless agreed to abide by RadioShack's previous privacy policies.[104] Once the Attorneys General, RadioShack, and General Wireless reached a settlement, Attorney General Paxton stated that the agreement reflected "a growing understanding of the importance of safeguarding customer information."[105]

The relevant case law and applicable Code provisions that address the sale of consumer information provide a glimpse into the approaches courts use when retailers file for bankruptcy. These procedures, however, only cover the fundamental actions courts take and do not delve into the broader preventative measures applied through ombudsman decisions, federal legislation, state laws, and independent privacy protection entities. Part III of this Comment will examine these measures in greater detail, address their limitations, and propose solutions to improve consumer privacy protection in retail bankruptcies.

II. ANALYSIS

A number of measures attempt to prevent the improper transfer of consumer information and the misuse of consumer information after it has been transferred in retail bankruptcies. This section first examines the privacy rights of consumers, the collection of consumer information, and the incentives for businesses to accumulate this information. Next, this section will explore current preventative measures used in retail bankruptcies and some of the limitations of these methods. Finally, this section will consider some of the potential solutions practitioners and other consumer protection advocates suggest, including a proposal for more federal oversight of consumer privacy that would directly impact the sale of consumer information in retail bankruptcies.

---

102 *See* Isidore, *supra* note 2; *see also* Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, ¶ 3.

103 *See* Debtors' Consolidated Reply in Support of IP Sale, *supra* note 2, ¶ 3.

104 *See* Isidore, *supra* note 2.

105 *Id*.

A. The Collection of Personally Identifiable Information

While the Constitution grants many enumerated rights, it does not explicitly grant a right to privacy to United States citizens.[106] Though not explicitly granted, American jurisprudence has expressed a general tort right to privacy as a "right to be let alone."[107] In 1965, the Supreme Court held, in *Griswold v. Connecticut*, that the individual rights conveyed by the Constitution include an implicit right to privacy in addition to those rights explicitly mentioned.[108] According to some commentators, "Our traditional view of privacy is premised on the autonomy of the individual and the idea that people should be free from intrusions into their personal lives."[109] The notion of a right to privacy becomes complicated when considered in conjunction with "informational privacy."[110] Informational privacy is the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[111] This form of privacy is much broader than the general right to privacy because it expands the concept of one's "self" to include digital information and virtual personality.[112] The right to informational privacy would place additional burdens and liability upon the collectors, holders, distributors, and purchasers of consumer information.[113]

The collection of consumer information is such a common practice in which businesses engage that it is hard to believe that more legislative and regulatory bodies have not implemented more effective regulations to monitor collection practices and consumer privacy.[114] To determine why broader

---

[106] John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH., no. 11, 2009, at 1, 6.

[107] THOMAS COOLEY, TREATISE ON THE LAW OF TORTS 389 (rev. students' ed. 1930); *see* Soma et al., *supra* note 107, at 6 (citing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890)); *see also* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 907 (2009).

[108] *See* Soma et al., *supra* note 107, at 5 (citing Griswold v. Connecticut, 381 U.S. 479 (1965)).

[109] *Id.* at 5.

[110] *See id.* at 6.

[111] *Id.* (citing Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. ¶ 1 (citing CHARLES J. SYKES, THE END OF PRIVACY 221 (1999))).

[112] *See id*.

[113] *See id*.

[114] *See generally* Miller, Jr. & O'Rourke, *supra* note 9, at 778; Nathan Newman, *How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population*, J. INTERNET L. 11, 12 (2014); *State Laws Related to Internet Privacy*, NAT'L CONF. OF ST. LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (last updated Jan. 5, 2016); *Privacy Law*, *supra* note 13.

federal privacy regulations may be necessary, one must first understand the details of consumer privacy and how collection practices make the security of consumer information more vulnerable. What information do businesses collect from consumers? Why is this information so valuable? Do consumers have a right to keep their information private when they willingly disclose it to businesses? The remainder of this subsection will explore answers to each of these questions.

Businesses gather a variety of information from customers, going far beyond the collection of names, addresses, and mere personal preferences.[115] In general, companies use consumer information to efficiently market products and services to consumers, which can lead to increased sales, revenue, and profits.[116] In fact, many companies are willing to purchase consumer information gathered by other businesses to improve their own consumer information collection efforts.[117] The collection of information can extend to a consumer's health, medical, and genetic data, financial and tax records, student information, publication purchases, viewed videos, retail transaction details, and even romantic and sexual preferences.[118]

Businesses tempt consumers to offer personal information in exchange for various benefits such as membership perks, online shopping convenience, personalization of frequented websites, and personalized advertisements.[119] In some instances, consumers provide personal information inadvertently through web tracking software.[120] Oftentimes, however, consumers are not completely aware of the consequences that come with revealing personal information.[121]

A large amount of consumer information businesses obtained originally came from third parties who solely compile information on over 700 million people from other public and private sources.[122] If businesses used this information inappropriately, consumers could potentially be harassed, embarrassed, blackmailed, discriminated against, stigmatized, or subjected to economic exploitation.[123] These risks are exacerbated each time PII is

---

115 *See* Thomson, *supra* note 11.
116 *See* Newman, *supra* note 115, at 11; Soma et al., *supra* note 107, at 10.
117 *See* Thomson, *supra* note 11.
118 *See id*.
119 *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 59 (1999).
120 *See* Miller, Jr. & O'Rourke, *supra* note 9, at 779.
121 *See generally* Killingsworth, *supra* note 120, at 59; Miller, Jr. & O'Rourke, *supra* note 9, at 782, 784.
122 *See* Thomson, *supra* note 11.
123 *See generally* Newman, *supra* note 115, at 11; Thomson, *supra* note 11, at 33, 34.

transferred from one business to another.[124] Bankruptcy courts have discovered prospective purchasers of consumer information that intended to sell and resell consumer information to anyone who would purchase it, including felons convicted of fraud.[125] Fortunately, courts have exposed these deceitful purchasers before the transfer of consumer information,[126] but these attempts illustrate how vulnerable a consumer's confidential information can be in retail bankruptcy asset sales.

The PII of consumers, which companies can sometimes obtain for a nominal value, "has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[127] The speed, ease, cost savings, and efficiency of electronic data have caused businesses to value, and even depend upon, digital consumer information considerably.[128] Companies rely upon the PII of consumers to reach and cater to their target audiences.[129] The use of targeted advertising and media outlets for marketing purposes translates into higher business revenues and reduced costs expended on uninterested consumers.[130] The impact that targeted advertising may have on business profits has generated a flourishing market for consumer information.[131]

In some cases, consumer information records are one of the company's most valuable assets.[132] For a company at risk of going out of business, consumer information records may be worth more than revenue from continued business.[133] In *In re RadioShack Corp.*, the court charged Hilco Streambank, an intellectual property consulting firm, to assess the retail debtor's consumer information records.[134] While serving as an intermediary for RadioShack, Hilco Streambank claimed that RadioShack had access to over 13

---

124 *See* Soma et al., *supra* note 107, at 2.

125 *See* Thomson, *supra* note 11, at 34.

126 *See id*.

127 Soma et al., *supra* note 107, at 2.

128 *See id.* at 9–10.

129 *See id*.

130 *See id* at 9.

131 *See id.* at 10.

132 *See* Miller, Jr. & O'Rourke, *supra* note 9, at 779; Steidtmann, *supra* note 9. *See generally* Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9.

133 *See* Martin D. Pichinson et. al, Committee Educational Session: Technology & Intellectual Property/Young and New Members IP Issues in Bankruptcy Deals: Monetizing IP: Variables Impacting the Value of IP Assets, *in* 042414 ABI-CLE 825 at 1 (Apr. 24, 2014).

134 *See* Topper et al., *supra* note 15. *See generally* About, HILCO STREAMBANK, http://www.hilcostreambank.com/about (last visited Jan. 11, 2016).

million email addresses and 65 million customer names and addresses.[135] Before the court's approval of the asset transfer, Hilco Streambank questioned whether the court would authorize a transfer of such a large magnitude.[136]

Most, if not all, consumers have some expectation of privacy when it comes to their PII because disclosure of the information could be harmful to them.[137] Studies have shown that most consumers are unaware of how retailers and other information collectors use PII.[138] Current privacy protections do not adequately provide surveillance over how businesses can use consumer information, especially because the uses are not always transparent to the affected consumers.[139] Surveys have shown that approximately 70% of consumers do not want to receive targeted advertisements or to have their search histories tracked.[140] Other consumers also have expressed concerns regarding the release of their information to third parties.[141]

Although current laws may not require a business to implement a privacy policy,[142] even when a business chooses to have a privacy policy in place, a consumer still has limited control over his or her PII.[143] If a retail customer wishes to file a claim for breach of a retailer's privacy policy, the customer may have few options available.[144] For instance, if a customer wanted to seek remedies against a retail debtor before the retailer's transfer of consumer information in bankruptcy, "the customer may be limited to a proof of claim unless the court grants the customer equitable relief or the customer can demonstrate gross negligence or recklessness on the part of the debtor's employees."[145] Oftentimes, consumers never file lawsuits because the "valuation of an individual's [PII] is not sufficiently high to offset the cost of litigation."[146] If a past retail customer sought remedies after that individual's information had been transferred, however, then "the customer may be eligible for damages against the debtor's estate and all breaching parties, including the

---

135 Brustein, *supra* note 2; Topper et al., *supra* note 15.
136 *See* Brustein, *supra* note 2.
137 *See* Misken & Simmons, *supra* note 39.
138 *See* Newman, *supra* note 115, at 17.
139 *See id.* at 12.
140 *Id.* at 17.
141 *See* Killingsworth, *supra* note 120, at 63–64; Newman, *supra* note 115, at 17.
142 *See Privacy Law*, *supra* note 13. *See generally State Laws Related to Internet Privacy*, *supra* note 115.
143 Newman, *supra* note 115, at 17.
144 *See generally* Committee Educational Session: Asset Sales/Technology and Intellectual Property, *supra* note 39, at 5.
145 Committee Educational Session: Asset Sales/Technology and Intellectual Property, *supra* note 39, at 5.
146 Soma et al., *supra* note 107, at 23.

employees."[147] Unfortunately, most consumers are incapable of fighting against dominating data collectors for the misuse of their private information.[148] This vulnerable position consumers often face requires additional privacy protections, especially under federal purview,[149] which would also apply in bankruptcy.

B. Preventative Methods and Their Limitations

Currently, there is an assortment of consumer privacy protection efforts by a variety of different administrations.[150] Much of the privacy protections available are offered through independently run privacy protection programs, state legislatures, and federal agencies.[151] While these key players have an interest in upholding consumer privacy, the majority of their efforts is ineffective in retail bankruptcies.

1. Oversight by Independent Companies

Many independent privacy programs monitor the exchange of consumer information within businesses and require adherence to minimum consumer privacy standards for program participation.[152] These privacy programs bring more credibility to consumer information collection practices by providing third-party evaluation and assessment of the practices.[153] Most of the privacy programs that exist today generally focus on monitoring online businesses and e-commerce.[154]

---

147 Committee Educational Session: Asset Sales/Technology and Intellectual Property, *supra* note 39, at 5.

148 *See* Newman, *supra* note 115, at 17.

149 *See id.* at 18.

150 *See, e.g.*, *supra* note 36 and accompanying text; 15 U.S.C. § 45(a) (2012); The Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2006); The Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996); The Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999); Seth Van Aalten, *Lessons from* RadioShack: *Selling Personally Identifiable Information in Chapter 11*, Committee Educational Session: Financial Advisors & Investment Banking/ Technology & Intellectual Property: You Are Selling My What? Valuation and Sale of Intellectual Property and Customer Information by a Distressed Company, 120315 ABI-CLE 141 n.40 (2015) (citing the consumer protection statutes of thirty-eight U.S. states and territories); THE BETTER BUSINESS BUREAU, https://www.bbb.org/boston/for-businesses/about-bbb-accreditation/advertising-bbb-accreditation/bbb-accredited-business-seal-for-the-web/ (last visited Nov. 4, 2015).

151 *See, e.g.*, text accompanying note 151.

152 *See generally* Killingsworth, *supra* note 120, at 65–66.

153 *See id.* at 65.

154 *See* Richard A. Beckmann, Comment, *Privacy Policies and Empty Promises: Closing the "*Toysmart *Loophole*," 62 U. PITT. L. REV. 765, 771 (2001).

Two of the most prominent privacy programs that monitor e-commerce include the Trusted Universal Standards In Electronic Transactions ("TRUSTe") and BBBOnLine, which is administered by the Council of Better Business Bureaus.[155] Businesses have an incentive to cater to online consumer privacy wishes because the e-commerce market allows for a faster preference response from privacy-conscious consumers.[156] In contrast, consumers are less likely to receive the same level of privacy protection through brick-and-mortar purchases.[157] Although the presence of online privacy evaluators can significantly improve the security of digitally-acquired consumer information, few independent privacy administrators exist to improve the security of brick-and-mortar consumer information exchanges.[158]

Even the diligent efforts of third-party programs, however, cannot offer complete protection of consumer information.[159] For instance, Toysmart.com had obtained a license agreement and privacy certification from TRUSTe before filing for bankruptcy.[160] One of the requirements TRUSTe set for Toysmart.com to receive the program's certification was to provide customers with notice and an opportunity to "opt-out" of the sale of their information before the proposed transfers occurred.[161] After learning that Toysmart.com intended to sell the consumer information it had collected through its website without informing or involving its customers, TRUSTe filed multiple objections with the bankruptcy court, including a request for the court to enforce the terms of the license agreement between Toysmart.com and TRUSTe.[162] Before Toysmart.com's voluntary withdrawal of the proposed transfer, TRUSTe's objections had not persuaded the court to prohibit the sale of consumer information without the consumers' consent.[163]

---

155 *See* MICHAEL D. SCOTT, SCOTT ON COMPUTER INFO. TECH. L. §16.33 (2016); Killingsworth, *supra* note 120, at 65–66. According to its website, TRUSTe describes itself as being an "independent, non-profit privacy initiative dedicated to building user trust and confidence on the Internet." *TRUSTe Sues Web Site for Unapproved Use of Privacy Seal Trusted Universal Standards in Elec. Transactions v. Underwriters Digital Research*, 18 ANDREWS COMP. & ONLINE LITIG. No. 4 R. 10 (2000).

156 *See* Beckmann, *supra* note 155, at 792; *see also* Killingsworth, *supra* note 120, at 62.

157 *See* Beckmann, *supra* note 155, at 770–71.

158 *See id.* at 771 n.40.

159 *See generally id.* at 781; *Truste Sues Web Site for Unapproved Use of Privacy Seal Trusted Universal Standards in Elec. Transactions v. Underwriters Digital Research*, *supra* note 156.

160 *See* Beckmann, *supra* note 155, at 768.

161 *See* Beckmann, *supra* note 155, at 769; *TRUSTed Data Program Requirements*, TRUSTE (July 20, 2016), https://download.truste.com/dload.php/?f=ADC1JZVZ-629 (last visited Dec. 31, 2016).

162 *See* Beckmann, *supra* note 155, at 769.

163 *See id.* at 768–69 (citing Obj. by TRUSTe to Mot. to Approve Stipulation, *In re* Toysmart.com, L.L.C., No. 00-13995-CJK (Bankr. E.D. Mass. filed Aug. 3, 2000)).

2. Oversight by State Laws

State Attorneys General have participated in bankruptcy cases to protect the privacy rights of consumers.[164] All fifty states have adopted consumer protection statutes prohibiting businesses from making deceptive representations to consumers, though these statutes vary in language and enforcement.[165] According to the National Conference of State Legislatures, "Ten states have constitutional provisions that expressly provide greater privacy protections than those provided for in the U.S. Constitution."[166] This notion appropriately recognizes the absence of an explicit right to privacy under the most authoritative law of the United States, as well as the disparate enforcement of privacy protections among the states.

When Congress delegates authority to the states to create their own policies within a given area, inconsistencies in the states' respective iterations of those policies are bound to ensue. The resulting "patchwork nature of privacy legislation" embodies this concept.[167] Legislative inconsistencies among state statutes only make it more difficult for businesses to properly abide by them.[168] For example, state laws differ on whether companies should be responsible for alerting consumers when their consumer information systems are breached.[169] Of the states that actually require companies to inform consumers of a breach, those provisions further vary on *when* a duty to inform consumers arises.[170]

In addition, only some state laws require businesses that participate in e-commerce to have privacy policies, and the enforcement of these laws varies among the states that have them.[171] Moreover, state privacy policy requirements are only likely to have an effect in bankruptcy proceedings if debtors seek relief in states where such laws are enforced.[172] In states where

---

164 *See* Thomson, *supra* note 11, 80.

165 *See* Van Aalten, *supra* note 151.

166 *Digital Privacy and Security: Overview of Resources*, NAT'L CONF. OF ST. LEGIS., (last updated Dec. 29, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/telecom-it-privacy-security.aspx.

167 Soma et al., *supra* note 107, at 22.

168 *See id.* at 28.

169 *See id.* at 29.

170 *See id*.

171 *See State Laws Related to Internet Privacy*, *supra* note 120 ("At least 17 states require government Web sites or state portals to establish privacy policies and procedures, or to incorporate machine-readable privacy policies into their Web sites.").

172 *See* Topper et al., *supra* note 15 ("Subject to bankruptcy court approval, the use, access, resale and dissemination of [PII] will occur with no customer consent. The only challenge exists in consumer protection statutes on a state-by-state basis.").

consumer privacy information protections are not enforced, the absence of federal privacy requirements increases the possibility that businesses will abuse consumer privacy protections.[173] Varied state consumer protection statutes also make it difficult to consistently and effectively hold retailers accountable for their actions when they inconspicuously sell consumer information.[174]

3. Oversight by Federal Legislation

Congress has used a "sectoral" approach when creating privacy regulations, which targets specific areas and industries.[175] This approach is "haphazard" and frequently overlaps or contradicts state privacy legislation.[176] Federal privacy legislation generally regulates within the private sector, specifically protecting the privacy of minors, healthcare information, and financial information.[177] Federal "sector" regulations impose strict limitations on the use of consumer information within the specific industries governed by the corresponding statute. These limitations would not apply in bankruptcy, however, unless the industry-specific form of information is pending a transfer. While there are some federal statutes that address specific consumer privacy concerns, they may have a limited application in retail bankruptcies.[178]

Perhaps one of the most pertinent federal statutes that has impacted privacy protections in bankruptcy proceedings is the FTCA.[179] Section 5(a) prohibits any "unfair or deceptive acts or practices in or affecting commerce."[180] The FTC considers an act deceptive if the conduct meets three criteria: (1) there is a representation, omission, or practice that (2) is likely to mislead consumers acting reasonably under the circumstances, and (3) the representation, omission, or practice is material.[181] In retail bankruptcies, violations of the

---

[173] *See id.* ("While under bankruptcy protection, however, there is less precedent and a much lower benchmark of consumer protection in adhering to privacy statutes.").

[174] *See id* ("Privacy policy use, application, adaptation, interpretation and enforcement are continually under question in business circumstances outside of bankruptcy court.").

[175] *See* Soma et al., *supra* note 107, at 23.

[176] *See id.* at 22.

[177] *See* The Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (1998); The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (1999); The Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

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

[179] *See* 15 U.S.C. § 45(a) (2012).

[180] *See id*.

[181] *See* Cliffdale Assocs., Inc., 103 F.T.C. 110, ¶ 37 (1984).

FTCA can occur if a retailer's sale of consumer information directly contradicts the retailer's privacy policy.[182]

If a retail debtor attempts to sell its consumer information to use the proceeds to pay off debts, and the retailer's privacy policy explicitly states that it will not sell consumer information to third parties, the FTC may intervene by claiming that the retailer intentionally misled its customers in violation of the FTCA.[183] In fact, the FTC used these same violations as its basis for objecting in *Toysmart.com* and *RadioShack*.[184] Though the FTC has persistently attempted to enforce these provisions and prevent unfair and deceptive practices in bankruptcy, the FTC's efforts have been limited to circumstances where a retailer violates its own privacy policy.[185] These efforts would be inapplicable in retail bankruptcies where the retail debtor did not have a privacy policy in place before filing for bankruptcy.

Appallingly, federal law does not require businesses to implement privacy policies or require businesses with existing privacy policies to inform customers of how they will handle consumer information.[186] This shortcoming further hinders the oversight that the FTC or any other federal government entity has over consumer information asset sales in retail bankruptcies. Because of the deficient federal directives subjecting companies to the responsible management and transfer of consumer information, some practitioners have advised companies to proactively avoid running into conflict with privacy policies, especially if their consumer information records are significantly valuable assets.[187] For example, a business could refrain from making any commitments to consumers that would restrict the sale of consumer information (because such a restriction could cause concern for the company's investors and creditors).[188] Other practitioners have advised businesses to clearly express in their policies that the company may freely transfer the PII of its consumers.[189] Though it is possible for some to question

---

[182] *See* Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9.

[183] *See id.*; Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

[184] *See* Press Release, Federal Trade Commission, FTC Requests Bankruptcy Court, *supra* note 5; Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

[185] Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

[186] *See generally Privacy Law*, *supra* note 13.

[187] *See* Brustein, *supra* note 2; Misken & Simmons, *supra* note 39, at 71.

[188] *See* Misken & Simmons, *supra* note 39, at 71.

[189] *See id*.

the soundness of such measures,[190] at least consumers would be aware of how businesses could potentially handle their personal information.

The Code is also a federally governed statute that could directly address privacy concerns in bankruptcy.[191] As previously mentioned in this Comment, § 363 of the Code urges retail debtors to maintain compliance with their privacy policies if they choose to sell consumer information during the bankruptcy process (even though the court can still approve a transfer in violation of the retail debtor's privacy policy in certain circumstances).[192] The Code, however, does not prevent a retail debtor from changing its privacy policy before filing for bankruptcy.[193] If a company chooses to alter its privacy policy before filing for bankruptcy, it may be able to avoid legal ramifications concerning the actual transfer of the consumer information.[194] Although there may be some form of recourse against the retail debtor under the FTCA for changing its privacy policy prepetition, any recourse under the FTCA may not impede the sale overall.[195]

The Code may, however, require the appointment of a consumer privacy ombudsman to investigate whether the transfer would violate nonbankruptcy law when a retail debtor attempts to sell consumer information.[196] Under §§ 322 and 363 of the Code, the consumer privacy ombudsman generally advises the court by providing the following information: (1) the debtor's privacy policy; (2) the potential losses, gains, costs, or benefits to consumers if the sale is approved; (3) the potential nonbankruptcy law violations if the sale is approved; and (4) any alternatives available to mitigate potential privacy losses or customer costs.[197] After reviewing the pertinent information, a consumer privacy ombudsman may recommend a variety of options to the court, including that: the purchaser of information be in the same business as

---

190 *See, e.g.*, Pat Conroy & Anupam Narula, *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry*, DELOITTE UNIV. PRESS (Nov. 13, 2014), https://dupress.deloitte.com/dup-us-en/topics/risk-management/consumer-data-privacy-strategies.html (discussing consumer preference for policies that promise to protect personal information).

191 *See* U.S. CONST. art. I, § 8, cl. 4.

192 *See* 11 U.S.C. § 363(b)(1) (2012).

193 *See generally id.* § 363.

194 *See generally id*.

195 *See* Committee Educational Session: Asset Sales/Technology and Intellectual Property, *supra* note 39 (noting the restrictions and potential violations that can occur if a retail debtor alters or abrogates its consumer information privacy policy prepetition).

196 *See* 11 U.S.C. §§ 332(a), 363(b)(1).

197 *See id*; Committee Educational Session: Asset Sales/Technology and Intellectual Property, *supra* note 39.

the debtor; the purchaser act as a successor to the debtor's privacy policies; the PII be sold either in conjunction with other assets or as a standalone asset; or the consumers have the opportunity to consent to or reject the transfer of their PII before the proposed transfer.[198] The ombudsman's role, however, is not to represent the interests of the consumers whose information stands to be transferred,[199] but to provide recommendations that assist the court in determining how to proceed with the sale.[200] After receiving the ombudsman's recommendation, a court may reject the suggestions offered.[201]

Research shows that out of the 400 bankruptcy cases since 2005 in which courts considered the appointment of a consumer privacy ombudsman, courts made appointments in only one out of every four cases.[202] In some instances, courts determined that there was no need to appoint an ombudsman if the purchaser of the consumer information agreed to abide by the retail debtor's privacy policy, regardless of the fact that the sale itself was against the debtor's privacy policy.[203] According to consumer privacy ombudsman Lucy L. Thomson, however: "This conclusion does not satisfy [bankruptcy policy], nor does it provide meaningful protection for consumers."[204]

Both creditors and debtors in retail bankruptcies would likely disfavor the appointment of an ombudsman because it causes a delay in the sale process and accounts for the subtraction of a large administrative expense from the retail debtor's estate.[205] Retail debtors likely do not have complete knowledge of the consumer information they possess, or knowledge of what information a retail debtor can sell to third parties.[206] Without the presence of an ombudsman in these cases, nonbankruptcy laws may be violated, there may be a lack of oversight on the purchaser's compliance to the retail debtor's privacy policies,

---

198 *See* Committee Educational Session: Asset Sales/Technology and Intellectual Property, *supra* note 39.

199 *See* Warren E. Agin, *Reconciling the FTC Act with the Consumer Privacy Ombudsman's Role*, 29 AM. BANKR. INST. J. 38, 89 (Oct. 2010).

200 *See id*.

201 *See* Miller, Jr. & O'Rourke, *supra* note 9, at 845.

202 Thomson, *supra* note 11.

203 *See id.* at 80; Van Aalten, *supra* note 151 ("While stopping short of an endorsement of the *Toysmart* resolution as a one-size-fits-all remedy to PII sales where the debtor's privacy policies (like RadioShack's) expressly pledge to not sell or transfer customer information to third parties, the FTC did acknowledge that its 'concerns about the transfer of customer information inconsistent with privacy promises would be greatly diminished' if the *Toysmart* conditions were met by RadioShack and the successful bidder.").

204 Thomson, *supra* note 11, at 80.

205 *See* Harmon, *supra* note 20, ¶ 20.07.

206 *See* Thomson, *supra* note 11, at 80.

and the sale procedure, consent process, or data disposal plans may be disorganized or inappropriate.[207]

While the collection and transfer of consumer information is on the rise, the efforts of independent privacy programs, state actors, federal administrations, and bankruptcy courts to safeguard the information have been insufficient. As important as it is for adequate and consistent enforcement of consumer privacy in bankruptcy, state and federal governments are only authorized to enact legislation outside of bankruptcy proceedings; within bankruptcies, government authority may be superseded by the judicial application of bankruptcy law.[208] The difficulties that the current protectors of consumer privacy face in bankruptcy courts demonstrate the need for the establishment of a comprehensive system that protects consumer information in bankruptcy.[209]

C. Proposed Improvements to Consumer Privacy in Bankruptcy

Many proposals have been offered to strengthen consumer privacy protection in retail bankruptcies.[210] One of these proposals is to "federalize"

---

[207] *See id*.

[208] *See* Beckmann, *supra* note 155, at 791.

[209] *See* Topper et al., *supra* note 15 ("Bankruptcy and liquidation proceedings should not preclude consumer protection violations and in particular privacy statutes. Data security for customer records is a ministerial function that should not be overlooked.").

[210] *See generally* Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9 (Commission Thompson stated, "Like my colleagues Commissioner Anthony and Commissioner Swindle, I think that consumers would benefit from notice and choice before a company transfers their information to a corporate successor . . . [customers should be provided] with notice and an opportunity to 'opt out' as a matter of good will and business practice"); Beckmann, *supra* note 155, at 787:

> The Attorneys General "urged the court to require that any buyer of the list notify customers of the transfer and seek their affirmative consent ("opt-in") to the continued use of their information . . . [TRUSTe argued for the court to] require the company to provide customers with notice and an opportunity to "opt-out" of the sale . . . the Massachusetts Attorney General claimed that the law of his state would require notice to and "opt-in" consent of the customers . . . [in a Texas settlement, the sale] could only proceed after customers were given notice and an opportunity to opt out."

Bellia, *supra* note 16, at 871, 874 ("[C]arefully crafted minimum privacy standards that cut across sectoral lines [would be] unproblematic, so long as such standards permit stronger sector- specific approaches . . . substantial consolidation in information privacy regulation would be a welcome development."); Schwartz, *supra* note 108, at 902 ("A broad coalition, including companies formerly opposed to the enactment of privacy statutes, has now formed behind the idea of a national information privacy law."); Topper et al., *supra* note 15 ("Patching the holes in easily identifiable scenarios such as bankruptcy is a surmountable solution that can end a massive data breach that has a ripple effect across payment processors, banks, insurers, retailers and software providers."); *Enterprise Privacy Certification Standards*, TRUSTE, https://www.truste.com/privacy-

minimum privacy regulations so that they are enforced across the United States in conjunction with sectoral and state regulations.[211] The centralization of privacy regulation within the federal context would impose broad privacy enforcement and ultimately override the bankruptcy court's discretion involving consumer privacy. Opponents of far-reaching federal legislation contend that the consolidation of privacy law under the federal sphere could lead to negative results, such as weaker state control and innovation over consumer privacy solutions.[212] Advocates of this approach, however, argue that broad legislation under the federal purview may be necessary to manage the range of harm and challenges that can arise from mishandling PII.[213]

Another option is to specify how consumer information asset sales should be handled within the Code.[214] This method is, arguably, another sectoral approach since it would narrowly apply to consumer protection within company bankruptcies and reorganizations.[215] With respect to retail bankruptcies, this approach may be an appropriate method to quickly react to a burgeoning threat in bankruptcy law.

1. Federal Direction and Expansion

Contrasting opinions exist as to whether privacy regulations should be administered federally, regionally, or sectorally. According to Paul M.

---

certification-standards/program-requirements/ (last visited Oct. 21, 2015) (requiring express consent of the customer prior to the sharing of sensitive information or the sharing of any personal information that is not in accordance with the company's privacy policy).

211 *See* Beckmann, *supra* note 155, at 791 ("Congress must act soon to create an equitable national standard that completely preempts state information privacy law."); Bellia, *supra* note 16, at 871, 874 ("[C]arefully crafted minimum privacy standards that cut across sectoral lines [would be] unproblematic, so long as such standards permit stronger sector- specific approaches . . . substantial consolidation in information privacy regulation would be a welcome development.").

212 *See* Schwartz, *supra* note 108, at 916.

213 *See* Bellia, *supra* note 16, at 871, 874 ("[C]arefully crafted minimum privacy standards that cut across sectoral lines [would be] unproblematic, so long as such standards permit stronger sector-specific approaches . . . substantial consolidation in information privacy regulation would be a welcome development."); *see also* Newman, *supra* note 115, at 12.

214 *See* Topper et al., *supra* note 15 ("Bankruptcy and liquidation proceedings should not preclude consumer protection violations and in particular privacy statutes. Data security for customer records is a ministerial function that should not be overlooked."); *see also* Beckmann, *supra* note 155, at 778–86, 790 (detailing the consumer protection inadequacies within the Code and attempted legislative responses to amend the Code).

215 *See* Killingsworth, *supra* note 120, at 71 ("Drafting a privacy policy means navigating a variety of United States statutes and legal principles of relatively narrow scope—a situation that has been described euphemistically as a 'sectoral' or 'layered' approach.").

Schwartz, a professor at the University of California, Berkeley, School of Law, a complete "Fair Information Practice" should include:

> (1) [L]imits on information use; (2) limits on data collection, also termed data minimization; (3) limits on disclosure of personal information; (4) collection and use only of information that is accurate, relevant, and up-to-date (data quality principle); (5) notice, access, and correction rights for the individual; (6) the creation of processing systems that the concerned individual can understand (transparent processing systems); and (7) security for personal data.[216]

Professor Schwartz also noted that "[n]o single privacy statute contains all these rules in the same fashion or form."[217]

In 2007, Bill Gates, along with many others, requested that the federal government impose uniform privacy standards by enacting comprehensive federal privacy laws to regulate the "collection, storage, and transfer of information across the private sector."[218] The enforcement of privacy legislation in the federal context could benefit consumers by diminishing the inconsistencies among state privacy laws.[219] In addition, the federalization of privacy regulations may curtail international conflicts that arise from unequal or potentially inadequate privacy policies, such as those between the United States and the European Union.[220]

There are possible drawbacks, however, that could arise with the federal administration of privacy. For example, federal privacy statutes could ostensibly preempt state privacy regulations[221] and result in weaker state control and innovation over consumer privacy solutions.[222] Further, businesses may resort to "defensive preemption," where businesses seek the passage of federal legislation to preempt state privacy laws with which they do not wish to comply.[223] Additionally, federal legislation can often take too long to enact because of congressional debate and gridlock.[224]

---

216 Schwartz, *supra* note 113, at 908.
217 *Id.*
218 *Id.* at 904.
219 *See id.* at 906 .
220 *See id.* at 904.
221 *See id.* at 917–18.
222 *See id.* at 920.
223 *See id.* at 905–06.
224 *See id.* at 917, 931.

These threats could potentially be alleviated with set "floors" or "ceilings" within federal privacy regulations, which would essentially set minimum and maximum standards for states to follow when enacting privacy laws.[225] For instance, Congress could set a floor that would require all businesses involved in the collection of information to have privacy policies in place that could improve the transparency of brick-and-mortar business usage of consumer information. The adoption of "baseline federal information privacy protections" allow states the flexibility and innovation to regulate consumer privacy, "while preserving sectoral protections that exceed the baseline, or . . . where there are gaps in sector-specific protection."[226] Thus, the expansion of federal privacy regulations—or at least the implementation of federal baseline standards—may prove to be a reasonable approach to ensure the security of consumer information privacy without excluding support from states and other consumer privacy advocates.[227]

2. Privacy Regulation within the Code

While the conditions created in the settlement agreements from *Toysmart.com* and *RadioShack* developed standards for the sale of consumer information in bankruptcy, FTC commissioners have criticized these standards as insufficient and inadequate.[228] Under certain circumstances, a retailer may have a greater responsibility to communicate with its customers than bankruptcy law requires. For example, in some states, retailers subject to data security breaches of consumer information are required to publicly acknowledge the breaches and to inform potentially affected customers.[229] Under these statutes, circumstances may call for a retailer to disclose breaches through written letters, emails, website postings, or media outlets.[230] In the settlement agreements drafted by the FTC in the *Toysmart.com* and *RadioShack* cases, the required terms did not include an obligation for either the seller or the buyer of the consumer information to notify customers of the

225 *See* Bellia, *supra* note 16, at 896–97. *Contra* Schwartz, *supra* note 108, at 919, 942–44.

226 Bellia, *supra* note 16, at 896–97.

227 *See id*.

228 *See* Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9.

229 *See* Jacob W. Schneider, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 283 (2009); *Security Breach Notification Laws*, NAT'L CONF. OF ST. LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

230 *See* Schneider, *supra* note 231, at 283.

sale.[231] Some critics have objected, however, arguing that consumer notification and/or consent should be required for retail debtors before transferring any data that contains PII.[232]

With respect to the settlement reached in *Toysmart.com*, Commissioner Anthony believed that "consumer privacy would be better protected by requiring that consumers themselves be given notice and choice before their detailed personal information is shared with or used by another corporate entity."[233] Likewise, although Commissioner Thompson approved the settlement in *Toysmart.com*, he urged for any purchaser of the information to "provide Toysmart customers with notice and an opportunity to 'opt out' as a matter of good will and business practice."[234] Commissioner Swindle stated that he would have voted in favor of the settlement had it "required that consumers affirmatively consent to have their information transferred to the purchaser, or, stated differently, had the transfer been conditioned on individuals' 'opting-in.'"[235] Additionally, in *RadioShack*, the Director of the FTC's Office of the Bureau of Consumer Protection stated in her letter to the consumer privacy ombudsman that a "consent process would allow customers to make their own determination as to whether a transfer of their information would be acceptable to them."[236]

Practitioners invested in consumer privacy protections have suggested an approach that would allow consumers "to participate in decisions on disclosure and use of their personal information, within a framework of data security and integrity."[237] Two key principles underlie this approach: (1) giving notice to consumers about how their information may be used; and (2) obtaining consent

---

[231] *See* Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4 (the buyer is only required to obtain affirmative consent from consumers if they materially change the privacy policy).

[232] *See generally* Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9 ("In my view, consumer privacy would be better protected by requiring that consumers themselves be given notice and choice before their detailed personal information is shared with or used by another corporate entity. . ."); Beckmann, *supra* note 155, at 769, 787 ("[The attorneys general] urged the court to require that any buyer of the list notify customers of the transfer and seek their affirmative consent ('opt-in') to the continued use of their information."); Topper et al., *supra* note 15 ("Just because a customer purchased a product at a point of sale or online does not necessarily assume they have opted in to be on a recurring distribution list, or for that data to be stored.").

[233] Press Release, Federal Trade Commission, FTC Announces Settlement, *supra* note 9.

[234] *Id.*; *see* 17-CM COLLIER ON BANKRUPTCY, *supra* note 31, ¶ 30.02.

[235] 17-CM COLLIER ON BANKRUPTCY, *supra* note 31, ¶ 30.02.

[236] Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4.

[237] Killingsworth, *supra* note 120, at 68.

from the consumer before using consumer information in a manner that is inconsistent with the methods communicated with the consumer.[238] This approach describes notice as the clear and accessible communication with consumers of the collection, use, and disclosure of their PII, and it describes consent as the consumers' choice to determine how their information should be used.[239]

There are two standard consent methods a business may choose when seeking approval from consumers to use consumer information in a manner outside of the normal course of business: (1) an "opt-in" approach; and (2) an "opt-out" approach.[240] Under the opt-in approach, consumers provide their consent by affirmatively choosing to allow a business to handle their information in a certain way.[241] Alternatively, under the opt-out approach, consumers deny their consent by indicating how or when they do not want their information handled.[242]

The FTC standards provided in *Toysmart.com* and *RadioShack* only require a retail debtor to obtain consent if the purchaser of the consumer information materially changes the seller's privacy policy.[243] On occasion, however, the bankruptcy court has used its discretion to require a consent process for the transfer of consumer information.[244] Generally, the application of a consent process in bankruptcy depends upon the sensitivity of the transferred information.[245] For example, after the electronics retailer Circuit City filed for bankruptcy in 2008, the court implemented an opt-out process recommended by the privacy ombudsman due to the involvement of over 47 million consumers in the case, which gained the attention of all fifty State Attorneys General.[246] Further, when the Texas online dating website, True Beginnings, filed for bankruptcy in 2013, the Texas Attorney General called for actual notice and an opt-in process before the sale of the retail debtor's consumer

---

238 *See id.* at 68–69.
239 *See id.* at 69.
240 *See id*.
241 *See id*.
242 *See id*.
243 *See* Letter from Jessica L. Rich, Dir. of the Bureau of Consumer Prot., Fed. Trade Comm'n, to Elise Frejka, Consumer Privacy Ombudsman for *In re RadioShack Corp.*, *supra* note 4 (stating that the buyer is only required to obtain affirmative consent from consumers if they materially change the privacy policy).
244 *See* Thomson, *supra* note 11, at 80.
245 *See id*.
246 *See id*.

information.[247] The bankruptcy court permitted the request.[248] The use of notice and opt-out procedures would "ensure that customers are aware that a new company will have access to their personal information, and . . . provide customers with the opportunity to choose not to deal with that company."[249]

Some practitioners have remarked that all businesses should employ individual notice and consent to ensure consumer privacy.[250] Conversely, other practitioners have suggested that the retailer cannot capitalize on the value of the information it possesses if forced to obtain notice and affirmative consent through opt-in or opt-out processes *before* transferring consumer information.[251] According to these practitioners, the consent process could diminish the value of the consumer information asset, thereby affecting the retail company's overall value.[252] This suggests that the devaluation would decrease the number of interested buyers, making it more difficult for a retail debtor to maximize the value of its assets, and thereby frustrating the principle of debtor rehabilitation.

These contrasting opinions illustrate the tensions between the desire for debtor relief and the protection of consumer privacy. Though the concerns of those who oppose mandatory notice and consent are not without merit, they do not acknowledge the need to find a balance between the principles of bankruptcy law with the interests of consumers.[253] Just as other sectoral approaches have deemed consumer privacy rights more important than a business's economic interests, the bankruptcy principle of maximizing the value of a retail debtor's estate should not preclude a consumer's right to informational privacy.[254]

CONCLUSION

Many factors prompt the stricter consumer privacy protections in retail bankruptcies, including the rise in the collection of consumer information by

---

247 *See* Nicole D. Mignone, *Privacy Protection for Dating-Website Customers*, AM. BANKR. INST. J. 16, 16, Apr. 2014; Thomson, *supra* note 11, at 80.

248 *See* Mignone, *supra* note 249, at 16.

249 17-CM COLLIER ON BANKRUPTCY, *supra* note 31, ¶ 30.02.

250 *See* Newman, *supra* note 115, at 19.

251 *See* Jones, *supra* note 8.

252 *See id*.

253 *See* Andrew Buxbaum & Louis Curcio, *When You Can't Sell to Your Customers, Try Selling Your Customers (but Not Under the Bankruptcy Code)*, 8 AM. BANKR. INST. L. REV. 395, 412 (2000).

254 *See* Topper et al., *supra* note 15.

retailers, the high probability that at least some retailers may file for bankruptcy, the likelihood that many of those retail debtors will attempt to sell valuable consumer information during bankruptcy, and the risks involved in the transfer of consumer information without consumer notification and consent. The security of consumer information will only become more fragile and complex in the future.[255] Although some methods are in place to thwart the abuse or neglect of consumer privacy protections, these measures alone do not sufficiently establish reliable and coherent procedures and standards for the sale of consumer information in retail bankruptcies. Stronger preventative measures, such as baseline federal privacy standards and explicit provisions in the Code, could improve the protections offered to consumers during the bankruptcy process.

One of the most effective methods suggested to strengthen consumer privacy protections is the establishment of baseline federal standards for all businesses that collect consumer information. Specifically, there should be a federal requirement that all businesses that gather consumer information establish privacy policies that will put consumers on notice of how businesses will handle their information after it is collected. Requiring businesses to implement privacy policies imposes minimal intrusion upon a state's enforcement of privacy laws because the state reserves the right to establish stronger controls over what a business may or may not do with the consumer information it collects. Further, businesses could still elect to have fewer restrictions on the use of information they collect as long as they inform consumers of their collection practices and those practices are within the bounds of the stronger state and sectoral privacy regulations. Requiring businesses to have privacy policies in place when consumer information is collected fills a critical gap in current state and sector privacy law enforcement and provides consistent enforcement of consumer privacy between online and brick-and-mortar retailers, as well as across state lines.

Though the establishment of minimum federal privacy standards would be an improvement to current consumer privacy enforcement, such standards may be insufficient to protect consumer information during the course of retail bankruptcies. To strengthen consumer privacy within the bankruptcy courts, the Code should contain further protections. Currently, §§ 322 and 363 of the Code allow for the broad discretion of a court to essentially override the promises a business makes to its customers in its privacy policy. To minimize

---

255 *See* Thomson, *supra* note 11, at 80.

the potential for abuse of consumer information and to provide adequate safeguards over consumer information sales, Congress should amend the language of §§ 322 and 363 to provide consumer ombudsmen with more authoritative oversight in cases where consumer information is exchanged and the bankruptcy court's broad discretion is reduced.

One measure that would improve consumer information transfers in retail bankruptcies is requiring the appointment of a consumer privacy ombudsman in any case where a business is likely to sell consumer information, even in cases where a purchaser promises to abide by the seller's privacy policy. Although the appointment of an ombudsman may add to the cost of the transfer, it is an effective way to hold purchasers accountable to the promises they make to induce the sale of consumer information. Further, retail debtors must comply with the guarantees they made to their consumers in their privacy policies, even during the bankruptcy process.

The fundamental bankruptcy principle of facilitating debtor rehabilitation should not outweigh a consumer's implicit constitutional right to privacy. When a transfer of consumer information would violate the business's privacy policy, the business should be required to inform its customers of the pending transfer, and in some circumstances, obtain the customer's opt-in or opt-out consent to the sale. Notice and consent procedures offer alternative methods in bankruptcy to facilitate the sale of consumer information while simultaneously preserving the bankruptcy principle of debtor rehabilitation. By requiring retailers to notify customers of their intentions to transfer consumer information and allowing customers the option to choose whether they want their information sold, consumers possess adequate control over their PII.

Placing privacy protections within the purview of federal legislation and the Code would establish a comprehensive approach to the sale of consumer information in bankruptcy courts, thereby significantly improving the protections offered to consumers. The FTC would have broader authority to prosecute businesses that blatantly disregard their own privacy policies. State Attorneys General can rest assured that the private information of his or her state's constituents is being handled in a manner that has been properly communicated to the consumers. Businesses will be aware of the potential implications of exchanging their customers' information with affiliate companies. Lastly, and perhaps most importantly, the control and delegation of

PII would place the information within the hands of whom it rightfully belongs.

KAYLA SIAM*

* Staff Member, *Emory Bankruptcy Developments Journal* (2016-18); J.D./M.B.A. Candidate, Emory University School of Law and Goizueta Business School (2018); B.A., *magna cum laude*, Governors State University (2014). First, I would like to thank Professor Sue Payne for offering her guidance during the writing process. Second, I would like to thank the staff members and editors of the *Emory Bankruptcy Developments Journal* for all of the editing and suggestions that helped to create a polished product that I could never have produced on my own. I would also like to thank my husband, Rashad Siam, for encouraging me in everything I set my mind to. Finally, I would like to thank my family, for I am merely a product of all of them, and I would be nothing without their love and support.