The New Regime for Treatment of Customer Data in Bankruptcy Cases

Warren E. Agin*

A telecom provider files a Chapter 11 case. Realizing its inability to reorganize on its own, it finds a buyer and files a plan of reorganization based on a sale of assets. All is well until the Federal Trade Commission files an objection. The objection alleges that the debtor signed-up approximately 1,000,000 subscribers using its Web site and its proposed sale, which includes subscribers' names, addresses, telephone numbers, and bank account information, violates the debtor's privacy policy. Faced with the possibility that the purchase will exclude a significant number of subscribers, a potential fight with the FTC, and a slurry of adverse publicity, the buyer backs out. Creditors are left holding the bag.

This scenario is not far from what occurred in the *Toysmart*[1] case last summer. In that case, described later in this article, the FTC and several state Attorney Generals opposed a debtor's attempt to sell customer data at auction. The result was a chilled sale and reduced recovery for creditors. *Toysmart*, although it did not result in a published opinion, illustrated the risks the bankruptcy process creates for both creditors and consumers when customer information collected on-line becomes involved in the bankruptcy process. This article will attempt to provide some background to the customer data privacy issue, describe the risks, review issues related to security interests in customer data, discuss proposed legislation to address the issues, and review options for dealing with the issues.

Consumer Data and Privacy in the New Century

On-line businesses collect several types of personal information. At the

---

* Warren E. Agin is a partner with Swiggart & Agin, LLC, an Internet and bankruptcy law boutique in Boston, Massachusetts. Chair of the ABA's Electronic Transactions in Bankruptcy Subcommittee, Mr. Agin is the author of BANKRUPTCY AND SECURED LENDING IN CYBERSPACE (Bowne, 2000).

[1] In re Toysmart.com, LLC, Case no. 00-13995-CJK, in the United States Bankruptcy Court for the District of Massachusetts.

@MAGNETO/MERCURY/PAMPHLET01/BANKRUPT/JOURNAL/WARREN SESS: 1 COMP: 05/18/01 PG. POS: 1

most basic level, they collect the same types of consumer information as any off-line business: such as a customer's name, address, telephone number and purchase history. More personal information is collected and retained. Transactional Web sites might retain credit card information, banking information, or even social security numbers. As in the off-line world, the business only collects this information when the customer provides it. But on-line businesses also collect information without the customer's knowledge. For example, many Web sites glean information about a visitor's computer and the visitor's activity on the Web site. The company uses this kind of information to customize the Web site to the visitor's needs and evaluate how well its Web site works. In the extreme, an Internet business can collect data about who you are and link it with information about what you do while using the Internet.[2]

Among on-line businesses, the trend is toward greater self-regulation of personal data and greater disclosure of how companies use collected data. The Federal Trade Commission and consumer protection groups encourage companies to self-regulate by adopting ''privacy policies.''[3] A privacy policy discloses an on-line business' data collection and use practices. Although privacy policies come in many different forms, the FTC and various consumer protection groups have developed recommended guidelines for privacy policies. These guidelines, referred to as ''fair information practices,'' describe what disclosures a privacy policy should contain and what companies should do to respect customer information.[4]

The typical privacy policy should do five things to follow fair information practices. First, it should give customers notice of what data the Web site collects and how the company uses the data. Second, it should give the customer a choice to ''opt-out'' of certain data uses. For example, a customer might be allowed to ask that the company not e-mail promotional materials about new products. Third, the company should give the customer access to his information and the ability to update or correct personal information. Fourth, the privacy policy should describe what steps the company takes to

---

[2] See, Jane K. Winn & James Wrathall, Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data, 56 THE BUSINESS LAWYER 213 (November 2000).

[3] More information about FTC initiatives in on-line privacy is available at <**www.ftc.gov/privacy/index.html**>.

[4] See *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress,* May 2000, available at <**www.ftc.gov/reports/privacy2000/privacy2000.pdf**>.

keep the personal information secure. Fifth, the company should provide a mechanism to allow customers to enforce the privacy policy.[5]

Some online companies contract with outside vendors like TRUSTe[6] or the Better Business Bureau Online[7] to review and validate their privacy policies. These companies will, assuming a Web site has an adequate privacy policy, let the company display a seal of approval. However, these companies will also provide an enforcement mechanism for consumers, creating a risk for the Web site that does not take its privacy policy seriously.

Concern over collection and use of personal information over the Internet is resulting in new information collection practices. New statutes restrict companies' ability to collect and use personal data in specific situations. COPPA: In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA)[8] to regulate collection of personal data by commercial Web sites that are targeted at children or that have actual knowledge that information is being collected from a child.[9] COPPA's provisions prohibit most collection of personal information from children unless the company first obtains verifiable parental consent. Even when consent is obtained, COPPA limits what data can be collected and how it can be used.[10] The Gramm-Leach-Bliley Act of 1999[11] and rules promulgated under that act by Federal agencies like the FTC,[12] control use of consumer data by financial institutions and govern their on-line privacy policies.[13] The Health Insurance

---

[5] Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 JOURNAL OF INTELLECTUAL PROPERTY LAW 57 (1999).

[6] <**www.truste.com**>.

[7] <**www.bbbonline.org**>.

[8] *The Children's Online Privacy Protection Act of 1998* (''COPPA''), 15 U.S.C. § 6501 *et seq*. (Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1998); implementing regulations at 16 C.F.R. Part 312 *et seq*.

[9] The term ''child'' is defined for purposes of the act as a person under 13 years of age.

[10] See, Marie G. Aglion, *Safety in the Virtual Playground: New Rules for Children's Web Sites*, 5 ELECTRONIC COMMERCE & LAW REPORT 358 (April 2000).

[11] 16 U.S.C. §§ 6801, et seq. (1999).

[12] Regulations issued by eight regulatory bodies (effective July 1, 2001): the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; FTC; SEC; National Credit Union Administration; Department of the Treasury. In addition, state agencies having regulatory authority over state chartered insurance companies are authorized to issue implementing regulations.

[13] See, John L. Douglas, *Gramm-Leach-Bliley Provisions Relating to Technology*, 4 ELECTRONIC BANKING LAW AND COMMERCE REPORT, No. 8 (February 2000).

Portability and Accountability Act of 1996 (HIPAA)[14] includes provisions requiring security procedures for electronic medical records.[15] The Fair Credit Reporting Act (FCRA)[16] may apply to on-line businesses that regularly collect and distribute to third parties personal financial information for credit or insurance underwriting or employment decisions.[17] The European Union Privacy Directive of 1995[18] governs the flow of personally identifiable information from EU member nations. It prohibits transfer of personal information to countries that do not provide ''adequate'' privacy protection. ''Adequate'' protection is not clearly defined by the Privacy Directive, but the United States does not currently qualify as a country providing adequate protection. The United States Department of Commerce has negotiated a set of ''safe-harbors'' for US companies to follow. A company complying with the safe harbor procedure and registering with the US Department of Commerce may import data from the EU without violating the Privacy Directive.[19]

In addition to statutes that specifically address the use of customer data, a company's use of customer data must also comply with section 5(a) of the FTC Act, which prohibits ''unfair or deceptive acts or practices in or affecting commerce.''[20] The FTC Act lets the FTC bring an enforcement action against a violator in Federal District Court. As it did in the *Toysmart* case, the FTC can sue in District Court despite the automatic stay.[21] State Attorney Generals have similar enforcement rights under state Consumer Protection Acts, which generally closely track the FTC Act. Filing a petition in bankruptcy does not absolve a debtor from complying with these statutes. The debtor's ability to use customer data when in bankruptcy remains the same

---

[14] 42 U.S.C. § 1320d (1996); final regulations at 65 Fed. Reg. 82462. See materials collected at: <**http://aspe.hhs.gov/admnsimp/final/FR010228.htm**>.

[15] See, Richard D. Marks, *Guidelines for Initiating HIPAA Systems Implementation Projects*, 5 ELECTRONIC COMMERCE AMP; LAW REPORT 468 (May 3, 2000).

[16] 15 U.S.C. § 1681.

[17] For in-depth information regarding the act, including enforcement actions undertaken by the FTC and the Commission's interpretive materials, see <**www.ftc.gov/os/statutes/fcrajump.htm**>.

[18] Council Directive 95/46, 1995 O.J. (L 281) 31. The Directive can be found at <**http://europa.eu.int/eur-lex/en/lif/dat/1995/en__395L0046.html**>.

[19] James A. Harvey & Karen Sanzaro, *Notes on Managing the Safe Harbor Privacy Requirements*, 5 ELECTRONIC BANKING LAW AND COMMERCE REPORT, No. 1 (May 2000); Scott Killingsworth & Brett Kappel, *Safe Harbor in Muddy Waters? Commerce Department Proposes Voluntary Principles for Compliance with EU Privacy Directive*, 1 E-COMMERCE LAW REPORT 2 (Dec. 1998/Jan. 1999).

[20] 15 U.S.C. § 45(a).

[21] The FTC can bring an enforcement action against a debtor in bankruptcy based on the police and regulatory power exception to the automatic stay. 11 U.S.C. § 362(b)(4).

as prior to the bankruptcy filing.[22] The debtor must also manage estate property according to the requirements of the valid laws of the States in which the property is located.[23] Thus, in addition to complying with Federal statutes specifically addressing the use and transfer of customer data, companies must consider the various positions of Federal and state agencies as to what practices they consider ''unfair or deceptive.'' Uniformly, these agencies consider ''unfair or deceptive'' a sale of customer data prohibited by a privacy policy.

Treating Customer Data as an Asset

The relationship between a customer providing data and the business using that data is not well defined, especially when the business collects the information subject to a privacy policy. To date, the practical issues have revolved around regulatory enforcement of privacy policies.[24] Treatment of customer data in bankruptcy cases also requires examining the debtor's right to the data as an asset of the estate[25] and whether the customer providing the data has a claim against the estate.

A company collecting customer data can assert a number of property rights in the data under different theories. First, information and data of a company constitutes a general intangible asset.[26] Second, if the data (a) has ''independent economic value'' so long as it remains a secret and (b) the company takes reasonable measures to keep the data a secret, the data might qualify as a trade secret, entitled to protection under state law.[27] Third, the database containing the information could be protected as copyrighted information, assuming the selection and arrangement of information within the database requires sufficient creativity.[28] As an asset, the trustee's ability to use, sell or lease customer data is governed by 11 U.S.C. § 363.

A privacy policy might be considered a contract between the customer

---

[22] Integrated Solutions, Inc. v. Service Support Specialties, Inc., 124 F.3d 487, 493, 31 Bankr. Ct. Dec. (CRR) 422, 38 Collier Bankr. Cas. 2d (MB) 805 (3d Cir. 1997).

[23] 28 U.S.C. § 959(b).

[24] See, Mark E. Budnitz, *Consumer Privacy in Electronic Commerce: As the Millennium Approached, Minnesota Attacked, Regulators Refrained, and Congress Compromised*, 14 NOTRE DAME JOURNAL OF LAW, ETHICS & PUBLIC POLICY 821 (2000). In the Matter of GeoCities, FTC File No. 9823015 (Feb. 12, 1999).

[25] See, Winn & Wrathall, *supra,* note 2.

[26] See, Id.

[27] Uniform Trade Secrets Act § 1(4), 14 U.L.A. 433 (1990 & Supp. 2000).

[28] Feist Publications, Inc. v. Rural Telephone Service Co., Inc., 499 U.S. 340, 111 S. Ct. 1282, 113 L. Ed. 2d 358, 18 Media L. Rep. (BNA) 1889, 18 U.S.P.Q.2d (BNA) 1275, 121 Pub. Util. Rep. 4th (PUR) 1 (1991).

and the company. In this case, would the contact be treated as executory?[29] Whether a privacy statement is executory or non-executory will depend on its terms, primarily whether it places continuing material obligations on each party.[30] The company will always have a continuing obligation to use and maintain data according to the policy's terms. Identifying a continuing material obligation of the customer is more difficult. Privacy policies tend to be one-sided and do not place any obligations on the customer. Occasionally, especially where the Web site integrates the privacy policy with an on-line contract, the customer might have a continuing material obligation to the company. However, Web sites usually contain separate privacy policies and terms of service.

Assuming the privacy policy is executory, a company desiring to retain customer data could always assume the privacy policy and continue to abide by its terms. Could a company that files a bankruptcy petition breach the use restrictions by transferring the data in violation of the contract, reject the contract, and leave individuals with general unsecured claims? A debtor rejecting a privacy policy might have to relinquish rights to data collected under the policy, but this presumes that the customer retains some kind of ownership interest or right in his personal data, a theory without current legal support.

A non-executory privacy policy would grant the customer even fewer rights. A debtor could breach the non-executory policy, and the customer's rights would be limited to a general unsecured claim. Possibly, a court might grant the customer the right to equitable relief against the debtor to prevent misuse of the provided information.

However, a privacy policy might not even qualify as an enforceable contract. One court has already stated that an on-line contract is not enforceable unless its terms are obvious and apparent, and that making the contract accessible only through a link at the bottom of a Web page does not qualify.[31] Using this reasoning, most privacy policies do not rise to the level of mutually enforceable contracts. In most cases, companies do not conspicuously display their privacy policy. A customer wanting to view the privacy policy must find and click on a small link at the bottom of a Web page.

Customer data held subject to rights of customers could potentially create a debtor-creditor relationship with the customer and give the customer a

---

[29] 11 U.S.C. § 365.

[30] Vern Countryman, *Executory Contracts in Bankruptcy, Part I*, 57 MINN. L. REV. 439 (1973).

[31] Ticketmaster v. Tickets.com, 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. 2000).

claim against the bankruptcy estate.[32] However, more likely the customer's remedies will be limited to the right to enforce the policy in equity allowing the debtor to exclude the customer, at least initially, from the class of creditors.

Treatment of Liens Against Customer Data

How does the relationship between the customer and business affect the lender? Generally, customer information, whether protected by Copyright law, maintained as a trade secret, or unprotected, is treated as a general intangible for purposes of Article 9. Attachment and enforcement of a lien against the customer data itself, or the proceeds from its sale, is relatively straightforward and well understood.[33] However, where the data is held and used subject to rights of the customer, whether contractual or pursuant to Federal or state law, those rights might limit the lender's ability to attach and enforce a lien against the customer data.

Current Article 9

Current Article 9 does not clearly address whether a contract or statute restricting transfer of customer data (or any general intangible) will preclude attachment of a security interest. At least one commentator has stated, ''existing law generally permits creation and perfection of security interests in otherwise nontransferable rights.''[34] Attachment, however, does not occur until the security interest becomes enforceable against the debtor with respect to the collateral.[35] Enforcement is conditioned upon (1) possession or execution of a security agreement, (2) giving of value, and (3) the debtor having rights to the collateral.[36] In some circumstances, as when the debtor has obtained or uses the customer data in violation of a statute such as COPPA or Gramm-Leach-Bliley, an argument can be made that the debtor

---

[32] Pursuant to 11 U.S.C. § 101(5), the customer will have a claim if it has a right to payment or an equitable remedy for breach of performance if such breach gives rise to a right to payment. However, it is not clear that a customer could have a monetary remedy for breach of performance under a privacy policy.

[33] With the caveat that perfection of a security interest in the data may require filing with the US Copyright Office where the data is protected under copyright law. See, Warren E. Agin, BANKRUPTCY AND SECURED LENDING IN CYBERSPACE, § 12.04[a] (Bowne & Co. 2000).

[34] Steven O. Weise, *The Financing of Intellectual Property Under Revised UCC Article 9*, 74 CHICAGO-KENT LAW REVIEW 1077 (1999).

[35] UCC § 9-203(2).

[36] UCC § 9-203(1).

lacks rights to the customer data and the lender's security interest thus fails to attach.

Presumably, even if the security interest attaches and is enforceable under current Article 9, the lender's ability to recover, use, or transfer the customer data will be subject to the applicable laws, regulations, and customer rights. For example, the lender's security interest will only attach to the information to the extent of the debtor's rights in that information, so, if legislation, such as Gramm-Leach-Bliley, limits the debtor's use of the data, that limitation will reduce the value of the collateral to the lender. Another example is where the debtor has contractually limited its rights to use or transfer the data. Then, the contractual restrictions will limit the scope of the security interest to those rights transferable by the debtor. In any case, transfer restrictions will limit the lender's ability to take possession of the collateral as an enforcement remedy and transfer the data to a third party.

Revised Article 9

Unlike current Article 9, Revised Article 9, in section 9-408, directly addresses the effect of transfer restrictions on general intangibles. Section 9-408 will apply in two circumstances. The first case is where the debtor holds the personal data pursuant to a term in an agreement that prohibits, restricts, or requires consent to assignment or transfer.[37] Where a privacy policy rises to the level of an enforceable contract, 9-408(a) will apply. Where a privacy policy does not rise to the level of an enforceable contract, 9-408(a) probably will not apply, because restrictive terms in the privacy policy will not qualify as a ''term . . . in an agreement.'' The second case is where a ''rule of law, statute or regulation'' prohibits, restricts or requires consent to assignment or transfer.[38] The consent required could be that of a governmental body or official or the consumer. Note that a privacy policy, statute or regulation that requires the consumer to ''opt-in'' before data can be transferred would clearly require consent. However, a policy, statute or regulation that merely requires that the consumer receive notice and have an opportunity to ''opt-out'' might not qualify as a provision that ''requires consent.''

Where 9-408 applies, either through subsection (a) or (c), the restrictive provision or legal requirement is ineffective to the extent it (1) would impair the creation, attachment, or perfection of a security interest or (2) provides

---

[37] Revised UCC § 9-408(a).

[38] Revised UCC § 9-408(c). None of the applicable statutes directly prohibit or restrict grant or attachment of security interests, and privacy policies themselves generally don't address the issue.

that the assignment or transfer of the data gives rise to a default, breach or remedy.[39] Thus, 9-408 provides a savings provision that allows creation and attachment of security interests in consumer data regardless of state law statutory or regulatory restrictions or contractual provisions contained in the privacy policy.

Section 9-408 has several limitations. Section 9-408(d) explicitly describes some of these limitations. Assuming the privacy policy or an applicable law prohibits assignment of the consumer data: the security interest is not enforceable against the consumer; the security interest does not impose a duty or obligation on the consumer; the lender can not use or assign the consumer information; the lender can not use, assign, possess or have access to any ''confidential information'' of the consumer; and the lender cannot enforce the security interest.

Thus, sections 9-408's savings provisions effectively are limited to letting the lender obtain a security interest for the purpose of recovering any proceeds either the debtor or a bankruptcy trustee generate from a sale of the data.

Section 9-408's application might be further restricted by the section's use of the term ''account debtor'' instead of the phrase ''other party to the agreement.'' An account debtor is ''a person obligated on . . . a general intangible.[40] However, customers generally have no performance obligation under a privacy policy. Thus, section 9-408(a)'s provisions may be generally inapplicable to promises made in a privacy policy. Section 9-408(c) may not apply to the extent that an applicable statute or regulation requires customer consent to a data transfer.

Another significant limitation of section 9-408 is its inability to render ineffective a Federal statute or regulation.[41] Since most of the statutory limitations on transfer of customer data, such as Gramm-Leach-Bliley, COPPA and the FTC Act, are Federal in nature, section 9-408 may not apply in most circumstances. However, the answer will depend on whether the provisions of section 9-408(c) are truly inconsistent with the relevant Federal laws given the exceptions contained in section 9-408(d), so that Federal preemption occurs.

Risk of Regulatory Action

---

[39] This is simplified of course. Section 9-408 is summarized here so as to emphasize its provisions most relevant to the discussion.

[40] Revised UCC § 9-102(a)(3).

[41] The Reporters' Comments to the 1998 Annual Meeting Draft stated ''This section does not override federal law to the contrary. However, it does reflect an important policy judgment that we hope will provide a template for future federal law reforms.''

Even where the lender's security interest attaches and is enforceable, the lender must consider the risk of regulatory action arising from either (1) the debtor's efforts to dispose of the customer information or (2) the lender's efforts to recover and dispose of the customer information. Where a regulatory agency having authority, whether the FTC or otherwise, believes the proposed action violates an applicable regulatory scheme, that regulatory agency could seek injunctive relief against the debtor or lender. The regulatory analysis will differ depending on whether the target is the debtor or lender. For example, the FTC's action against Toysmart was based on the argument that Toysmart's attempt to sell customer data was an unfair or deceptive business practice because it violated the promise Toysmart made to its customers. However, a hypothetical lender to Toysmart would not be a party to that promise. Would a lender's effort to recover and sell the data violate the FTC Act? Perhaps it would, but not for the same reasons.

The lender's very involvement could implicate regulatory schemes not applicable to the debtor. For example, a debtor based in Europe might fully comply with the EU Data Directive, but its US based lender's recovery of the data might violate the EU Data Directive. An interesting question is whether circumstances exist where customer data could become subject to GLB upon recovery of the collateral data by a lender. A retail seller that accepts credit cards or checks, or sells goods on layaway, is not subject to Gramm-Leach-Bliley, but its lender would be with respect to certain customers if the lender takes over the credit facility operations.

Missteps in this area could cause loss of valuable collateral, adverse regulatory activity, and negative public relations. A lender dealing with customer data collateral needs to think out the regulatory environment before acting. However, where a potential problem exists creative solutions can always be found.

The Problem Realized: Toysmart.com and Living.com Case Studies

Historically, few rights attached to corporate use of personal data. What rights did exist were provided solely by statute. In the traditional framework, a company in bankruptcy can use customer data without restriction. It also can sell the data freely, either as part of the entire business, or separately. In some cases, the customer data is one of the most valuable assets. Companies, by using privacy policies, change the traditional treatment provided customer information. Federal and state agencies may insist on continued compliance with promises made in the privacy policy, and compliance with Federal, state and foreign laws governing use and transfer of customer data.

In re Toysmart.com, LLC[42] involved an actual sale of customer data. Toysmart operated an on-line toy store that ran into financial trouble and ceased operations in May 2000. Toysmart had, in 1999, adopted a privacy policy and become a licensee of TRUSTe. Toysmart's privacy policy stated that Toysmart would not share its customers' data with third parties. After its creditors filed an involuntary Chapter 11 case against it, Toysmart filed a motion to conduct a public auction of several assets, including its customer data. On learning about the proposed sale of personal information, TRUSTe complained to the FTC that the proposed sale would violate Toysmart's privacy policy. The FTC sued Toysmart in Federal District Court alleging that the sale of data was an unfair or deceptive business practice violating the FTC Act, and requesting the court enjoin the sale.[43] The FTC also asserted that some of the customer data was collected from children in violation of COPPA. The FTC's action forced the company to limit its sale options in order to settle the complaint. The company agreed to sell the information only to a family-oriented buyer that agreed to abide by Toysmart's privacy policy and the company filed a motion seeking bankruptcy court approval of the settlement.

However, several State Attorney Generals objected to the proposed auction. Their objection asserted that the sale, even if conducted subject to the conditions of the FTC settlement, constituted an unfair or deceptive business practice in violation of the states' consumer protection statutes. Faced with only one bid, by Disney Corporation, and active opposition from the state Attorney Generals, the debtor withdrew the customer data from the auction. In the end, one of Toysmart's major investors, Disney Corporation, paid the debtor $50,000 for the debtor to destroy the customer data, rather than transfer it.

When Living.com, Inc., an on-line furniture retailer, filed a Chapter 11 case in August 2000,[44] the Texas Attorney General raised concerns over the company's treatment of customer data. Living.com had a privacy policy that stated that ''. . . living.com does not sell, trade or rent your personal information to others without your consent.'' Even though no sale of the data was pending, the Texas Attorney General threatened legal action to protect consumers from any possible violation of their rights. Rather than litigate, Living.com entered into a settlement agreement with the Texas Attorney General. Under the agreement, Living.com's bankruptcy trustee agreed to destroy customers' personal financial data, such as credit card information,

---

[42] In re Toysmart.com, LLC, Case no. 00-13995-CJK, in the United States Bankruptcy Court for the District of Massachusetts.

[43] *FTC v. Toysmart.com, LLC*, civil case no. 00-11341-RGS (D. Mass., filed 7/10/00).

[44] *In re Living.com, Inc.*, Case. 00-12522, US Bankruptcy Court for the Western District of Texas.

and to give customers notice and an opportunity to ''opt-out'' of a sale before selling their personal data.[45] This meant that before the trustee could sell the data he would have to inform customers of the proposed sale and, if the customers so requested, remove their personal information from the data being sold.

The Current Legislative Solution: The Leahy-Hatch Amendment

The *Toysmart* and *Living.com* cases illustrate the difficult problems raised by the sale of customer data in a bankruptcy case. On the one hand, allowing a sale of data in violation of a privacy policy might constitute an unfair and deceptive business practice and thus violate both Federal and state law. On the other hand, enforcing an overly restrictive privacy policy might prevent an otherwise reasonable sale of customer data to the detriment of creditors. Currently, the Bankruptcy Code lacks an efficient mechanism for balancing these interests. The Bankruptcy Code also lacks a viable mechanism for protecting consumer interests in this context. The FTC and state Attorney Generals cannot be expected to monitor all business bankruptcy cases and intervene on behalf of customers every time a debtor attempts to sell customer data. The customers themselves may lack the right to enforce the privacy policy, and raising all customers to creditor status raises its own obvious problems.

The Leahy-Hatch Amendment adding sections 231 and 232 to S. 420, The Bankruptcy Reform Act of 2001, addresses these issues. It creates a framework to allow sale of ''personally identifiable information'' while protecting customer's interests. ''Personally identifiable information,'' is limited to specific types of information ''provided by the individual to the debtor in connection with obtaining a product or service from the debtor primarily for personal, family, or household purposes.''[46] These items are:

1. The individual's first name (or initials) and last name;
2. The individual's physical home address;
3. The individual's e-mail address and home telephone number;
4. The individual's social security number or credit card account number; and
5. when identified with one or more of the above items, the individual's birth date, birth certificate number, place of birth or any other information concerning the individual that, if disclosed, will result in the physical or electronic contacting or identification of the individual.

---

[45] *Cornyn Announces Privacy Settlement with Living.com*, (Official Press Release) viewed at <**www.oag.state.tx.us/newspubs.releases/2000/20000925living.com.htm**> September 25, 2000.

[46] Bankruptcy Reform Act of 2001, § 231 (b).

Section 231 limits the sale or lease of ''personally identifiable information'' under 11 U.S.C. § 363 where the debtor has disclosed a privacy policy prohibiting the information's transfer to unaffiliated third parties and the policy remains in effect at the time of the bankruptcy filing.[47] Thus, while a debtor may be able to revise its privacy policy pre-petition, changes made to a Chapter 11 debtor's privacy policy during the case will not change its ability to sell or lease customer data. Also, section 231 does not restrict a debtor's ability to use customer data under section 363, so long as that use does not constitute a sale or lease.

When section 231 applies, the trustee can only sell or lease the personally identifiable information under two circumstances. First, when the sale is consistent with the privacy policy's prohibitions on transfer. Second, when the Court, after appointment of an ombudsman, notice and hearing and due consideration of the facts, circumstances, and conditions of the sale or lease, approves the sale or lease.[48] Thus, the court has discretion to allow a sale or lease in violation of the privacy policy.

Section 231 does not provide a standard for the court to follow in allowing a sale or lease inconsistent with a privacy policy, however section 232 requires appointment of an ombudsman to assist the court in its decision. When a trustee wants to sell customer data in a manner inconsistent with the applicable privacy policy, it must first request that the court order appointment of an individual to serve as ombudsman. The court must enter such order not later than (a) thirty days after the order for relief or (b) five days prior to any hearing on the sale of customer data.[49] How the time periods will work in practice is actually not very clear from the text of the statute. Most likely, the trustee will file a request for appointment with the sale motion. Because section 232 does not grant the court discretion to deny the request, the order authorizing appointment would be automatic in most cases.[50] The US Trustee actually appoints the ombudsman, who must be a disinterested person other than the US Trustee. Hypothetically, the ombudsman could be an FTC commissioner or state Attorney General.[51] The ombudsman shall be entitled to notice of, and have a right to appear and be heard, at the sale hear-

---

[47] The Bankruptcy Reforms Act of 2001, § 231(a).

[48] Id.

[49] The Bankruptcy Reforms Act of 2001, § 232(a).

[50] The court might deny the request for appointment where it denies the sale motion without hearing.

[51] Although the court might consider these individuals ''interested'' because of their clear mandate to enforce their respective consumer protection statutes.

ing,[52] shall maintain as confidential any ''personally identifiable information'' he receives,[53] and shall be compensated in the same manner as an examiner.[54] The ombudsman is not entitled to employ his own professionals.

The ombudman's role is not explicitly to represent consumers, but to provide the court information to assist the court in deciding whether to allow a non-conforming sale or lease of ''personally identifiable information.'' The statute does not dictate the nature of this information, but suggests that the information might include a presentation of the applicable privacy policy, potential loses or gains of privacy to consumers if the sale or lease is approved, potential costs or benefits to consumers of the sale or lease, and potential alternatives to the sale which would mitigate potential privacy losses or potential costs to consumers.[55] In short, the ombudsman appears more of an expert commentator than a consumer advocate, but the act implies the ombudsman's role is to ensure consumer protection.

Handling Customer Data in the Bankruptcy Case

Given the new regulatory oversight of bankruptcy sales of customer data, counsel will have to examine more closely the role customer data will play in each bankruptcy case. The first issue will always be the existence and terms of a privacy policy. Did a privacy policy exist? What promises or statements were made in the privacy policy? Did the policy state data would never be shared or did it give the customer notice that the information might someday be transferred? Are reservations by the company of the right to transfer data clear and conspicuous? Was the privacy policy itself displayed in a clear and conspicuous manner? The best practice is for customers to have had a chance to review and indicate acceptance of the entire privacy policy: but the best practice is rarely the followed practice. The company may have used more than one version of the privacy policy raising the question of which privacy policy governs the customer's rights. The task of linking customer information to the applicable privacy policy can create a significant problem.

Before attempting to sell customer data in an insolvency situation, the company should assess whether the data was legally collected and held. Data collected or used in violation of COPPA, GLB or any of the other applicable statutes could, if sold, result in legal action by the FTC or other regulatory agency. Even if the initial transfer of the data escapes notice, the

---

[52] The Bankruptcy Reform Act of 2001, § 232(a)(3).

[53] The Bankruptcy Reform Act of 2001, § 232 (a)(4).

[54] The Bankruptcy Reform Act of 2001, § 232 (c).

[55] The Bankruptcy Reform Act of 2001, § 232 (a)(2).

purchaser may become subject to future regulatory action by purchasing the customer data.

Determining whether the company's customer data collection and use policies comply with the technical requirements of statutes like COPPA requires analyzing the policies in light of the applicable regulations. Determining whether a proposed sale of data would constitute an unfair or deceptive business practice violating the FTC Act is harder.

In *Toysmart*, the FTC took the position that because the privacy policy promised not to share the data with third parties, any sale of the data would be an unfair or deceptive business practice. However, that position is not supportable. For example, Toysmart regularly shared customer data with the shipping companies hired to deliver toys. Although that practice violated the letter of its privacy policy, it inarguably was neither unfair nor deceptive. On the other hand, Toysmart's selling its customer data to mass marketers might be an unfair or deceptive business practice even if its privacy policy were cleverly drafted to allow the sale. Whether a given sale of customer data violates the FTC Act should depend on many factors including the terms of the privacy policy, the identity of the buyer, restrictions on the buyer's use of the data, whether the buyer will continue to abide by the privacy policy, and the customers' expectations about how the company would use the data.

The company might consider methods for transferring customer data, or customers, designed to reduce the risk of regulatory action. For example, the FTC and most state Attorney Generals have indicated they would find acceptable a process where the customer data is only sold after the customer is informed of the sale and affirmatively agrees to it. This process is referred to as ''opt-in,'' because the customer must affirmatively opt-in to the sale before his customer can be sold. This process should reduce almost all risk of regulatory action. Unfortunately, it will in most cases also greatly reduce the amount of data actually transferred.

An alternative method, called ''opt-out,'' gives the customer notice of the proposed transfer and, before the transfer, gives the customer a chance to affirmatively ''opt-out'' of having his information transferred. Because this method does not require the customer to affirmatively act in order to allow the information transfer, it will increase the amount of data the company can sell. However, some state Attorney Generals will object to ''opt-out'' procedures.

Once the Bankruptcy Reform Act of 2001 becomes effective (assuming it does and also assuming the Leahy-Hatch Amendment remains in the final version) the trustee (or DIP) should consider requesting early appointment of an ombudsman. Appointment of an ombudsman should reduce the risk that the FTC or a state Attorney General employs early intervention to protect consumers. The ombudsman can also work with the trustee to

structure appropriate sale guidelines so the trustee can offer the customer data on terms it knows the ombudsman will support. The trustee does not want to propose a sale and then find out, after the fact, that the appointed ombudsman's recommendations to the court don't support the sale. On the other hand, the trustee does not want to overly limit his sale options to terms he is absolutely positive the court will approve. By providing a degree of comfort with sale terms, an ombudsman can help the trustee maximize his recovery from sale of customer information. This is especially true where a privacy policy completely prohibits sale of customer data.

Where the buyer does not just want the data, but is trying to acquire the failed company's customers, methods exist that allow a ''transfer'' of data without actually transferring it. For example, the selling company might agree to forward the buying company's marketing materials to the customer list for a price, rather than release the customer list. Another possibility is for the selling company to refer customers to the buying company. The buying company pays a fee either for each customer referred, or for each customer that actually purchases goods or services from the buying company.

The *Toysmart* case illustrated the issues surrounding the sale of customer data subject to privacy policies. Now that practitioners have seen what can happen, the problems the debtor faced in *Toysmart* are avoidable. All that's required is proper planning and an appreciation for customer rights. The Leahy-Hatch Amendment will help address the issue by providing a workable framework to let the courts balance rights of creditors and customers. Thus, while selling customer data will require greater attention in future cases, practitioners should be able to avoid the kind of controversy that erupted in the *Toysmart* case.