18 Midwest L. Rev. 43

Midwest Law Review
Winter, 2002

WEB PRIVACY POUCIES AND OTHER ADVENTURES IN NEVER NEVER LAND

Jordan M. Blanke[a1]

Mercer University

INTRODUCTION

When you register with toysmart.com, you can rest assured that your information will never be shared with a third party.[1]

Like penny candy, nickel packs of baseball cards and quarter hot dogs, they just don't make "never" like they used to. When toysmart.com advertised its customer list for sale in the Wall Street Journal the day before a bankruptcy proceeding against it was commenced, a new generation of Internet privacy questions was introduced: How enforceable are Web privacy policies, and who is going to enforce them? How long is "never" in Bankruptcy Court? And is it true that you should never say "never" again, at least in your privacy policy?

TOYSMART.COM

On May 22, 2000 Internet retailer toysmart.com announced that it was ceasing to do business. It began soliciting bids for the purchase of its assets. On June 8, it advertised for sale in the Wall Street Journal its databases and customer lists. On June 9, toysmartxom's creditors filed a petition for involuntary bankruptcy. On June 19, toysmart.com informed the Federal Trade Commission that it would not transfer its customer lists without bankruptcy court approval.

On July 10 the FTC instituted an action against toysmart.com seeking an injunction preventing the transfer of any of toysmart.com's customer lists to any third party, and declaring any such transfer to be a violation of Section 5 of the FTC Act.[2] That section prohibits "unfair or deceptive acts or practices in or affecting commerce."[3] The FTC has authority to enforce violations of the Act by instituting proceedings seeking injunctive and other equitable relief.[4]

The FTC complaint[5] alleges that toysmart.com collected on its Website personal customer information including names, addresses, billing information, shopping ***44** preferences and family profile information. The list supposedly contains such personal information on 190,000 people who registered with and/or made purchases from toysmart.com.[6] The complaint also alleges that since September 1999 toysmart.com had a privacy policy posted on its site stating that:

> 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.[7]

On July 21 the FTC announced that it had reached an agreement with toysmart.com governing any transfer of the customer lists to a third party.[8] Under the agreement toysmart.com would sell or assign the lists only as part of a sale of the entire Web site to a "qualified buyer" approved by the bankruptcy court.[9] A qualified buyer would be an entity whose business was concentrated in the "family commerce market, involving education, toys, and/or learning."[10] It was agreed that any such qualified buyer would be bound by toysmart.com's privacy statement and responsible for any violations of it after the date of transfer. It was further agreed that if the qualified buyer were ever to materially change the privacy statement, those changes would not apply to the original information unless the individual who provided the information specifically and affirmatively agreed to the new

policy (i.e., the individual would have to "opt-in"[11]).

The FTC voted 3-2 to approve the settlement Commissioner Shelia F. Anthony dissented, refusing to put business interests ahead of consumer privacy. She stated that since consumers had provided personal information pursuant to a promise not to share it with any third party, they should be given notice of any transfer and the option to share their information.

Commissioner Orson Swindle also dissented, emphasizing the promise toysmart.com had made to its customers:

> If we really believe that consumers attach great value to the privacy of their personal information and that consumers should be able to limit access to such information through private agreements with businesses, we should compel businesses to honor the promises they make to consumers to gain access to this information ... In my view, such a sale should not be permitted because "never" really means never.[12]

***45** Commissioner Mozelle W. Thompson approved the settlement but said that he, like his colleagues, still had some reservations about it. He pointed out that in building its customer database, its principal remaining asset, toysmart.com had made a covenant with its customers not to transfer the information. He was convinced, however, that the settlement agreement is consistent with toysmart.com's privacy policy and that the information would be adequately protected. He stated that he hoped any successor to the customer lists would provide those on the lists "with notice and an opportunity to 'opt out' as a matter of good will and good business practice."[13]

Despite FTC approval, the attorneys general of about 40 states opposed the settlement agreement, believing that the it did not go far enough in enforcing toymart.com's promise and protecting privacy. They wanted toysmart.com to notify its customers beforehand of any potential sale of the lists, and to allow any customer to opt out.

On August 17 the Bankruptcy Court of the Eastern District of Massachusetts rejected the settlement agreement. Judge Carol Kenner noted that there was much opposition to the proposed settlement, and that it was premature to restrict the terms of a sale when there were not even any concrete offers. The decision was made without prejudice to the parties' raising these issues again if and when a prospective buyer were ever found.

Finally on January 26, 2001, the Bankruptcy Court approved the sale of the list to the Buena Vista Internet Group (BVIG), a subsidiary of Walt Disney Co. and a majority shareholder of toysmart.com.[14] BVIG agreed to purchase the list for $50,000 and have it destroyed by attorneys for toysmart.com without ever seeing or handling the list. This unusual action was taken to avoid any further negative publicity about the list.

OTHER DOT-COMS

Ever since Craftshop.com became the first Internet retailer to declare bankruptcy and offer its customer database for sale, privacy advocates, lawyers and businesses have paid close attention to this new area of controversy. Like toysmart.com, Craftshop.com had very strong language in its privacy policy:

> We will hold your secure online shopping information in the strictest confidence ... We will *never* release it to any person or any company for any purpose. We do not sell, rent or lend any part of our mailing list[15]

Craftshop has taken the position that as long as a buyer uses the list under the Craftshop name, there is no violation of its privacy policy. Former Craftshop CEO Angus Mackey stated that since it had promised not to release the names ***46** without approval, it would sell the company name and the customer list together.[16]

On August 29, 2000, Internet furniture retailer living.com filed for protection under Chapter 11 of the Bankruptcy Code. The Texas Attorney General sought an injunction preventing the sale of its customer lists and personal financial information, living.com's privacy policy stated that:

> living.com does not sell, trade or rent your personal information to others without your consent. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank email to never @living.com.[17]

The parties entered into a settlement agreement, under which the court-appointed bankruptcy trustee would oversee the destruction of customer personal financial data such as credit card, bank account and social security numbers. The trustee would be authorized to sell or transfer the rest of the information in the customer list as long as notice is given to each customer with an opportunity to opt out of the proposed sale or transfer. The bankruptcy judge would have to approve the notice and opt-out form sent to the customers. The bankruptcy judge has not yet approved the settlement agreement.[18]

In September 2000, the U.S. Bankruptcy Court for the Southern District of New York approved the sale of the assets of bankrupt APBnews.com to Safetytips.com. Included was a list of e-mail addresses of customers who requested free news updates. APBnews.com's privacy policy did not promise *never* to share or sell the information it collected. As a result, there was not as much controversy over this sale.

OTHER REACTIONS

Two major pieces of legislation have already been introduced in the Senate in this new privacy battlefield. In May Senator Ernest F. Hollings introduced a bill, the Consumer Privacy Protection Act, that would amend the Bankruptcy Code to exclude from property of the estate any personally identifiable information or compilation thereof. It would require affirmative consent before a Website could collect or disclose personally identifiable information, and would also require affirmative consent after any material change is made to a privacy policy.[19]

In July 2000 Senator Patrick J. Leahy introduced a bill, the Privacy Policy Enforcement in Bankruptcy Act of 2000, that would similarly amend the ***47** Bankruptcy Code to exclude from property of the estate any personally identifiable information whose sale or disclosure would violate the privacy policy in effect at the time the information was collected.[20]

Possibly the most significant response was Amazon.com's posting of a new Privacy Notice over the Labor Day weekend. In it Amazon.com made clear that it shares customer information with its subsidiaries and affiliated businesses. It also added a section called Business Transfers:

> As we continue to develop our business, we might sell or buy stores or assets. In such transactions, customer information generally is one of the transferred business assets. Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.[21]

Before the policy change, customers had the option of sending an e-mail to never@amazon.com to forbid Amazon.com from selling, renting or trading personal information to a third party.[22] Now customers' only "opt-out" choice is with respect to promotional offers from other businesses.[23]

Another important change is Amazon.com's declaration that its privacy policy will inevitably change, and that "use of information that we gather now is subject to the Privacy Notice in effect at the time of use."[24] This assertion will certainly be challenged at some point in time.[25] Many customers who have disclosed personal information based upon specific representations about how it will be used will not be happy to learn that Amazon has unilaterally decided to change those promises.

Two major privacy advocacy groups, Electronic Privacy Information Center and Junkbusters, terminated their affiliate relationships with Amazon in protest over these changes. Both published letters on the Web explaining why they were so disappointed in Amazon's weakened privacy protection.[26]

*48 THE NEXT GENERATION OF QUESTIONS

How Enforceable are Web Privacy Policies, and Who Is Going to Enforce Them?

The FTC has been involved with privacy issues on the Internet for several years. For the past three years, it has produced annual reports that have become cornerstones of the efforts to shape and define privacy protection on the Web.[27] The FTC has been at

the center of a variety of privacy-related issues, including enforcement of the Children's Online Privacy Protection Act, and investigation into online profiling. It has clearly become one of the leaders in the efforts to protect personal information and privacy on the Web.

The FTC is an independent federal agency created by statute.[28] It is authorized to enforce Section 5(a) of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[29] It may initiate proceedings in federal district court to enjoin violations of the FTC Act and to secure appropriate equitable relief.[30]

In its first Internet privacy case in 1998, the FTC challenged the data collection practices of one of the largest and most popular sites on the Web. The FTC alleged that GeoCities was deceiving its customers about how it was using personal information collected on its site. Specifically, the FTC alleged that GeoCities was disclosing information (such as education level, income, marital status, occupation and interests) to third parties despite its promise to the contrary.

In a settlement agreement,[31] GeoCities agreed to post a clear and prominent privacy policy on its site, informing consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. GeoCities agreed not to misrepresent the purpose for which it collects or uses personal identifying information. It also agreed to notify its members and provide them with an opportunity to have their information deleted from its database.

***49** In addition to the action against toysmart.com, the FTC also commenced (and settled) actions in the last year alleging unfair or deceptive trade practices against ReverseAuction.com,[32] and against Worldwidemedicine.com and Focusmedical.com.[33]

Many state attorneys general have also become active in the enforcement of privacy-related fair trade practices on the Web. As discussed above, over 40 attorneys general objected to the proposed settlement agreement in the toysmart.com case. Also discussed above is the quick action taken by the Texas Attorney General to prevent the sale of customer information by the bankrupt living.com.[34]

The Attorney General of Missouri recently brought suit against more.com, an Internet health care and nutrition product retailer, alleging that it disclosed personal information to third parties despite promises in its privacy policy that the information would not be shared.[35] Attorney General Jay Nixon stated that:

> Web sites should not be selling consumers' personal information to other businesses when the site's privacy policy clearly states that information won't be shared to others ... Consumers have a right to be upset when the companies giving them assurances of privacy and non-disclosure are not keeping their word.[36]

Protecting individual privacy on the Web promises to be one of the important legal and consumer issues of the next few years. It will probably become a factor in some political races. In Texas, Attorney General John Cornyn boasted in his press release about the living.com case that his office was the first to file an objection in bankruptcy court to the proposed sale of the toysmart.com customer lists.[37] He promised to "continue to vigorously fight any proposed future sale ... without adequate notice and consent to Texas consumers."[38]

The FTC and the state attorneys general are ready and willing to use whatever powers they have to enforce promises made online. It certainly appears that they will fervently pursue breaches of these promises as unfair and deceptive trade practices.

***50How Long Is "Never" in Bankruptcy Court?**

Bankruptcy courts will be venturing into relatively uncharted waters as they confront the question posed in the toysmart.com case: Can a customer list compiled with specific representations of privacy be sold without regard to those promises?

While the court in the toysmart.com case did not have to answer this question since a sale was never consummated, it will certainly resurface in some case in the near future. As more and more dot.coms file for bankruptcy, courts will be faced with the same situation.

In many of these bankruptcies, the customer lists or customer database will be the most significant asset of the estate. The bankruptcy courts, while charged with assuring that the assets of the estate be maximized, will have to decide if these lists can be sold, and if so, whether any restrictions will attach.

Several sections of the Bankruptcy Code are relevant. Section 105[39] gives the court considerable power to fashion an appropriate legal or equitable remedy. While courts will no doubt examine a variety of other sections, they may very well return to this one to use fairness as the guiding principle upon which to base a decision.

Under section 541, the estate of the bankrupt is comprised generally of all legal and equitable interests of the debtor in property as of the commencement of the proceeding.[40] While this definition of property is very broad and has been so interpreted, there will be questions as to whether any restrictions on the debtor's property (e.g., promises made about not disclosing certain information to others) will be applicable to the trustee in bankruptcy and any subsequent transferor.

Section 541(c) states that an interest of the debtor in property becomes property of the estate notwithstanding any provision in an agreement, transfer instrument, or applicable nonbankruptcy law that restricts or conditions the transfer of such interest.[41] There have been numerous cases, however, holding that this section does not give the estate any greater rights than the debtor had.

***51** In *Butner v. U.S.*,[42] a case that is often cited by those cases interpreting the scope of section 541, the Supreme Court held that one looks to state law to determine the nature and extent of a debtor's interest in property, and transfers such interest intact to the estate. Subsequent cases have interpreted this to mean that "[s]uch interests are not enlarged, enhanced, or altered,"[43] that "Section 541(a) does not give to the estate more than the debtor possessed at the time of the filing,"[44] and that "only those property rights which are owned by the debtor become the bankruptcy estate."[45]

In *In re Sanders*,[46] the Seventh Circuit summarized this area of the law, stating
The ... decision is founded on the basic tenet of bankruptcy law that a bankruptcy trustee succeeds only to the title and rights in property that the debtor had at the time she filed the bankruptcy petition ... Filing a bankruptcy petition does not expand or change a debtor's interest in an asset; it merely changes the party who holds that interest ... Further, a trustee takes the property subject to the same restrictions that existed at the commencement of the case. "To the extent an interest is limited in the hands of a debtor, it is equally limited as property of the estate."[47]

Perhaps the reported case most on point is *Rice v. Shoney's, Inc. (In re Dean)*.[48] In that case, the debtor was an employee of Shoney's, who along with other Shoney's employees and their employer invested in a joint venture in some Captain D's restaurants. The joint venture agreement specifically limited any transfers of interest to only Shoney's or its employees.

The court held that while the debtor's property did become part of the estate, the restrictions on transfers remained enforceable. It stated
The purpose of section 541(c)(1)(A) was to permit the transfer of the debtor's interest to the estate, notwithstanding any restriction on that transfer ... Thus, section 541(c)(1)(A) does not invalidate the restrictions in ***52** the joint venture agreement. Rather, it ensures that the debtor's interest in that joint venture agreement, including transfer restrictions imposed upon the debtor not otherwise precluded by law, becomes property of the estate.[49]

The court held that the trustee was bound by the same restrictions that the debtor had been, and that the property rights were not expanded simply by virtue of the fact that the property was part of the estate. It held that the "trustee succeeds to all of the rights of the debtor, including restrictions on transfers."[50]

There is certainly a convincing argument here that restrictions on the use of the information collected by a company in creating its customer database should similarly be respected. Just as Shoney's and its employees who invested in the joint venture in the Rice case may have had reasons for restricting ownership to that group, individuals deciding to disclose personal information based upon representations of privacy may not have done so absent those assurances. This line of cases certainly provides strong support for the position that the nature of the property should not change or expand merely because it becomes part of an estate in bankruptcy.

Sections 363[51] and 704[52] of the Bankruptcy Code enable the trustee to sell property of the estate and collect the proceeds therefrom. Several cases have addressed the question of whether the trustee has greater rights than the debtor to transfer property. In *In re Schemer*,[53] the court held that it did not:

> ***53** [T]here is no conflict between 11 U.S.C §§ 363(b)(1), 704, and state law which defines the debtor's rights in property of the estate. Sections 363(b)(1) and 704 do not expressly authorize the trustee to sell property contrary to the restrictions imposed by state and contract law. These sections are simply enabling statutes that give the trustee the authority to sell or dispose of property if the debtors would have had the same right under state law.[54]

Similarly, in *Integrated Solutions, Inc. v. Service Support Specialties, Inc.*,[55] the court held that sections 363 and 704 are general enabling provisions and do not expand or change a debtor's interest in property merely because it files a bankruptcy petition. It cited *Butner* and its progeny,[56] as well as *Schauer* and subsequent cases holding that a trustee's rights are not enlarged beyond those that the debtor had before filing.[57]

Even if a customer list or customer database becomes property of the estate,[58] a bankruptcy court could easily enforce the restrictions thereon. It could impose the same restrictions on the trustee that were on the debtor prior to filing for bankruptcy.

A bankruptcy court has already decided one case involving privacy and a customer database. In *In re Cult Awareness Network, Inc.*,[59] the debtor was an organization that tracked the activities of groups it considered to be cults. It maintained a database that contained names of individuals believed to be involved with them. The trustee received offers as high as $75,000 for the database. However, there were threats from individuals whose names were in the database to sue for invasion of privacy if their names were disclosed. The trustee wished to abandon the database, fearing that potential costs of defending lawsuits would cost more than could be realized from a sale. The court permitted the trustee to abandon the property even though it had some value, holding that it was within the trustee's discretion to decide that the ultimate cost to the estate might be outweighed by its benefits.

As suggested above, until a legislative solution appears (if one appears), a bankruptcy court might feel most comfortable relying on its broad powers to fashion an equitable remedy.[60] When personal information is collected from individuals with a promise that it will *never* be disclosed, a court might very well determine that never does in fact mean never. As was suggested by many state ***54** attorneys general in the toysmart.com matter,[61] it would be very easy to require that individuals be given an opportunity to opt out, or even, opt in.

Should You Use the Word "Never" in Your Privacy Policy?

Legally, it would appear that you would be better off not to use the word "never" (or words with similar meaning) in your privacy policy. Because it is such a definite term, there is a very strong argument for the FTC or an attorney general, or a trustee or a bankruptcy court that "never" should mean never. We have already seen this to be true in some of the cases discussed above.[62]

However, if the numerous opinion polls showing how important privacy has become to the typical Web user are to be believed,[63] we may see more companies aggressively market their privacy policies. We have already seen some companies take strong measures to enforce their policies.[64]

Organizations are deciding whether to adopt "opt-in" or "opt-out" privacy policies. An opt-out policy puts the burden on the consumer to request *not* to be included in the data collection. Typically, a Website has a series of check boxes that are "checked" by default. If a user wishes not to receive offers, solicitations or email from the site, or from its "partners" or "associates," he must uncheck the box. Otherwise, by default, he will receive them. This type of opt-out policy is the most prevalent on the Web today.[65]

***55** In an opt-in policy, if a consumer wishes to receive those same offers, solicitations or email, she has to take the affirmative step of checking the check box. Otherwise, by default, she will not receive them, and according to most such policies, she will not be placed on any customer list or in any database. We are beginning to see more and more companies consider this

alternative.[66] Some companies are using both approaches; some information will be collected unless the individual chooses to opt out, while other choices may require opting in.

Companies may decide to keep the word "never" in their privacy policies for a variety of reasons. They may do so because they believe it is the right or ethical thing to do. They may do so because they really don't need the information in their business. They may do so to distinguish themselves from competitors. Whatever the reason, they must realize that they may very well be held to their promise.

We will certainly continue to see changes in the environment in which these policies exist. Technology will change the manner in which, and the type and quantity of, information that can be collected.[67] New laws will dictate how, when, why and what information can be obtained.[68] Market and social pressures ***56** will also influence decisions made about how much privacy will be expected or how little tolerated.

Ultimately a business will have to gage the environment in which it operates to adopt an appropriate policy. In the near future, it is unlikely that the legal environment will require or prohibit the word "never." More likely, consumer demands and competitive responses will determine its prevalence.

Footnotes

a1 Professor of Computer Information Systems and Law, Stetson School of Business and Economics, Mercer University, Atlanta, Georgia

1 Privacy Statement of toysrnart.com, *available at*htro:// www.ftc.gov/os/2000/07/toyexhl.pdf

2 15 U.S.C. § 45(a).

3 *Id*.

4 *Id*. at § 53(b).

5 *Available at*http://www.ftc.gov/os/2000/07/toysmartcmp.htm. A First Amended Complaint, adding a claim alleging violations of the Children's Online Privacy Protection Act, was subsequently filed, and is *available at*http:// www.ftc.gov/os/2000/07/toysmartcomplaint.htm.

6 Michael Brick, *Judge Overturns Deal on Sale of Online Customer Database*, N.Y. TIMES, Aug. 18, 2000, *available at*http:// www.nytimes.com/2000/08/18/technology/18toys.html.

7 *Supra* note 1 (emphasis added). The Privacy Statement also contained the language found in the text accompanying note 1.

8 FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations, July 21, 2000, http:// www.ftc.gov/opa/2000/07/toysmart2.htm.

9 Stipulation and Order Establishing Conditions on Sale of Customer Information, http://www.ftc.gov/os/2000/07/toysmarttbankruptcy.1.htm.

10 *Id*.

11 *See infra* notes 65-66 and accompanying text

12 Dissenting Statement of Commissioner Orson Swindle, http:// www.ftc.gov/os/2000/07/toysmartswindlestatement.htm.

13 Statement of Commissioner Mozelle W. Thompson, http:// www.ftc.gov/os/2000/07/toysamrtthompsonstatement.htm

14 In re Toysmart.com, LLC, No. 00-13995-CJK (Bankr. D. Mass. Jan. 26, 2001).

15 The Craftshop.com Website is no longer accessible, but its privacy policy is quoted in *Failed Dot-Corns May Be Selling Your Private Information*, N.Y. TIMES, July 1, 2000, *available at*htrp:// www.nytimes.com/2000/07/01/technology/01info-selling.html (emphasis added).

16 *Id*.

17 *See* Press Release, Office of the Attorney General, State of Texas, Cornyn Announces Privacy Settlement with Living.com (Sept 25, 2000), http:// www.oag.state.tx.us/newspubs/releases/2000/20000925*l*iving.com.htm

18 *Id.; see* Notice of Settlement with Attorney General (Sept 25, 2000), *at*http://www.living.com

19 S. 2606, 106th Cong. (2000), *available at*http:// thomas.loc.gov/cgi-bin/bdquery/z?d106:s.02606:.

20 S. 2857, 106th Cong. (2000), *available at*http:// thomas.loc.gov/cgi-bin/bdquery/z?d106:S.2857:.

21 Amazon.com Privacy Notice, *at*http:// www.amazon.com/exec/obidos/tg/browse/-/468496/104-8882782-9729549

22 Tamara Loomis, *Amazon Revamps Its Policy on Sharing Data*, N.Y. LAW JOURNAL, Sept. 21, 2000, at 5.

23 Amazon.com Privacy Notice, *supra* note 20.

24 *Id*.

25 Both Senate bills that propose modification of the Bankruptcy Code recognize that potential problems may arise when privacy policies are changed, and contain restrictions. *see supra* notes 18-19 and accompanying text.

26 Letter from Marc Rotenberg, Executive Director, Electronic Privacy Information Center, to EPIC Subscribers (Sept 13, 2000), *at*http:// www.epic.org/privacy/internet/amazon/letter.html; letter from Jason Catlett, Junkbusters, Inc., to Jeff Bezos, Chief Executive Officer, Amazon.com, *at*http://www.junkbusters.com/ht/en/amazon.html. Andrew Shen, Policy Analyst at EPIC, testified before the House Commerce Committee on Recent Developments in Privacy Protection for ConsuMers on Oct 11, 2000, and spoke about his concern over recent attempts of bankrupt companies to auction off their customer databases and his dismay about Amazon.com's new privacy policy. The Prepared Testimony and Statement for the Record of Andrew Shen is *available at*http:// www.epic.org/privacy/internet/shen_testimony_1000.html

27 In 1998 the FTC made its first comprehensive report to Congress, *Online Privacy: A Report to Congress*, *at*http://

www.ftc.gov/reports/privacy3/index.htm. It followed that in 1999 with *Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress, at*http://www.ftc.gov/os/1999/9907/index.htm#13, and in 2000 with *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress, at*http:// www.ftc.gov/os/2000/05/index.htm #22. In its first two reports, the FTC had advised Congress that efforts at industry self-regulation was progressing well and would be sufficient to protect the privacy interests of consumers. In its last report, it switched positions, and advised Congress that it needed to take legislative action in order to protect those interests.

[28] 15 U.S.C. § 41 (2000).

[29] *Id*. at § 45(a).

[30] *Id*. at § 53(b).

[31] *See* Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information, August 13, 1998, http:// www.ftc.gov/opa/1998/9808/geocitie.htm

[32] *See* Online Auction Site Settles FTC Privacy Charges, January 6, 2000, http://www.ftc.gov/opa/2000/01/reverse4.htm. The FTC sued an online auction house for illegally collecting personal information from another Web site, and using that information to solicit business from those individuals.

[33] *See* Online Pharmacies Settle FTC Charges, July 12, 2000, http:// www.ftc.gov/opa/2000/07/iog.htm. The FTC sued a group of online pharmacies that advertised facilities that they did not actually have and made promises about consumer privacy and confidentiality that they did not keep.

[34] *See supra* notes 16-17 and accompanying text.

[35] *See* Press Release, Office of the Missouri Attorney General, Web Site Violated Law by Giving Out Personal Information to Third Parties After Stating it Would Not, Nixon Says (Sept. 14, 2000), http:// www.ago.state.mo.us/091400.htm

[36] *Id*.

[37] *Supra* note 16.

[38] *Id*.

[39] 11 U.S.C. § 105(a) (2000).

[40] 11 U.S.C. § 541 (2000). §541(a) provides, in part, that:
The commencement of a case under section 301, 302, or 303 of this title creates an estate. Such estate is comprised of all the following property, wherever located and by whomever held:
(1) Except as provided in subsections (b) and (c)(2) of this section, all legal or equitable interests of the debtor in property as of the commencement of the case

[41] 11 U.S.C. § 541(c) (2000). §541(c) provides in part, that:
(1) Except as provided in paragraph (2) of this subsection, an interest of the debtor in property becomes property of the estate under subsection (a)(1), (a)(2), or (a)(5) of this section notwithstanding any provision in an agreement, transfer instrument, or applicable

nonbankruptcy law--
(A) that restricts or conditions transfer of such interest by the debtor; or
(B) that is conditioned on the insolvency or financial condition of the debtor, on the commencement of a case under this title, or on the appointment of or taking possession by a trustee in a case under this title or a custodian before such commencement, and that effects or gives an option to effect a forfeiture, modification, or termination of the debtor's interest in property.
(2) A restriction on the transfer of a beneficial interest of the debtor in a trust that is enforceable under applicable nonbankruptcy law is enforceable in a case under this title.

42 440 U.S. 48 (1979).

43 *In re*Shoen, 193 B.R. 302 (Bankr. D. Ariz. (1996).

44 *In re*Stephen Smith Home for the Aged, Inc., 80 B.R. 678 (E.D. Pa. 1987).

45 *In re*Transcon Lines, 58 F.3d 1432 (9th Cir. 1995), *cert. denied sub nom.*, Gumport v. Sterling Press, Inc., 516 U.S. 1146 (1996).

46 969 F.2d 591 (7th Cir. 1992).

47 *Id*. at 593 (citations omitted). *See also*Integrated Solutions, Inc. v. Service Support Specialties, Inc., 124 F.3d 487 (3rd Cir. 1997); *In re*FCX, Inc., 853 F.2d 1149 (4th Cir. 1988).

48 174 B.R. 787 (Bankr. E.D. Ark. 1994).

49 *Id*. at 789-790.

50 *Id*. at 791.

51 11 U.S.C. § 363 (2000). §363 provides, in part, that
(b)(1) The trustee, after notice and a hearing, may use, sell, or lease, other than in the ordinary course of business, property of the estate.
...
(f) The trustee may sell property under subsection (b) or (c) of this section free and clear of any interest in such property of an entity other than the estate, only if--
(1) applicable nonbankruptcy law permits sale of such property free and clear of such interest;
...
(l) Subject to the provisions of section 365, the trustee may use, sell, or lease property under subsection (b) or (c) of this section, or a plan under chapter 11, 12, or 13 of this title [11 USCS §§ 1101 et seq.,1201 et seq., or 1301 et seq.] may provide for the use, sale, or lease of property, notwithstanding any provision in a contract, a lease, or applicable law that is conditioned on the insolvency or financial condition of the debtor, on the commencement of a case under this title concerning the debtor, or on the appointment of or the taking possession by a trustee in a case under this title or a custodian, and that effects, or gives an option to effect, a forfeiture, modification, or termination of the debtor's interest in such property.

52 11 U.S.C. § 704 (2000). §704 provides, in part, that
The trustee shall--
(1) collect and reduce to money the property of the estate for which such trustee serves, and close such estate as expeditiously as is compatible with the best interests of parties in interest;
(2) be accountable for all property received;

[53] 835 F.2d 1222 (8th Cir. 1987).

[54] *Id*. at at 1225.

[55] *Supra* note 46.

[56] *Supra* notes 41-49.

[57] *See In re* FCX, Inc., *supra* note 46; *In re*Bishop College, 151 B.R. 394 (Bankr. N.D. Tex. 1993).

[58] As discussed above, there are two Senate bills pending that would exclude from property of the estate any personally identifiable information collected with assurances of privacy. *See supra* notes 18-19 and accompanying text.

[59] 205 B.R. 575 (Bankr. N.D. Ill. 1997).

[60] *See supra* note 38 and accompanying text.

[61] *See supra* notes 2-13 and accompanying text.

[62] *See supra* notes 1-17 and accompanying text.

[63] See Jeff Sovem, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999). Professor Sovern cites numerous opinion polls that generally show that there is great concern for consumer privacy. *Id.* at 1057-1066. He also discusses why some studies show that consumers may not be availing themselves of opportunities to protect their personal information as much as one might expect *Id*. at 1067-1093.*See also* Bob Tedeschi, *Sellers Hire Auditors to Verify Privacy Policies and Increase Trust*, N.Y. Times, Sept. 18, 2000, *at*http://www.nytimes.com/2000/09/18/technology/18ECOMMERCE.html (citing a survey by the Odyssey research firm that found that 92 percent of online households do not trust online companies to keep their information private, no matter what they promise).

[64] *See* Tedeschi, *supra* note 62. Two online companies, Expedia and E-Loan, hired Big Five accounting firm PricewaterhouseCoopers to conduct extensive audits of their online privacy policies. Both are interested in convincing reluctant consumers that they are true to their stated privacy policies. E-Loan paid PricewaterhouseCoopers a reported $250,000 for the initial audit, plus an additional $30,000 for each quarterly audit.

[65] During the last few years, industry has pushed for the self-regulation of privacy on the Internet Spurred chiefly by the threat of new legislation, many organizations have adopted privacy policies. These efforts have been well documented by the FTC in their annual reports to Congress, *supra* note 26. Also driving self-regulation have been the negotiations between the Department of Commerce and the European Commission. After about three years of negotiation, a safe harbor agreement was finally approved, and took effect in November 2000. Under the agreement, American organizations can guarantee a free flow of information between the United States and European Union countries by agreeing to abide by certain provisions regarding privacy policies and data protection. Amid a good bit of opposition from the European countries, where protection of personal information is much more heavily regulated, the cornerstone of the agreement is self-regulation. Generally speaking, organizations must post a privacy statement that addresses the core principles of notice and choice, and self-regulate their adherence to those policies. Except for "sensitive data," which includes things like race, religion, ethnic origin and political beliefs, an organization need only provide an individual with an opportunity to opt out While this is a vast oversimplification and would have many exceptions running in each direction, one might characterize the European system as "opt-in" and the American system as "opt-out." *See* Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, ___ ALB. L.J. SCI. & TECH. ___ (2000).

66 *See* Tom Weber, *To Opt In or Opt Out: That is the Question When Mulling Privacy*, THE WALL STREET JOURNAL, October 23, 2000 at B1. While most companies still want to keep their opt-out policies, PricewaterhouseCoopers privacy expert Larry Ponemon advises clients to seriously consider opt in policies. "There are real business advantages. Consumers are starting to view privacy as a loyalty ingredient," he said. *Id.*

67 *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, (1999). Professor Lessig describes how behavior is effected by four modalities of regulation in both real space and cyberspace: law (e.g., the law prohibits the sale of certain drugs), social norms (e.g., where it is appropriate to smoke), markets (e.g., the price of gasoline may limit the amount that one drives), and architecture (e.g., a highway dividing two neighborhoods may limit the extent to which they integrate). The architecture of cyberspace is its code, the hardware and software from which it is constructed. Lessig discusses how this code can displace law. For example, in copyright law, we are used to having a book that can be read over and over again. What if we had an "electronic book" that came with a limited number of times you could read it? Might not this provide better protection for this intellectual property? He also discusses how law can regulate code. For example, laws have already been passed that require code to limit the number of times that a copy can be made from a DAT tape, that prevent the circumvention of code designed to prevent access to digital material, and require the use of a V-chip capable of recognizing different kinds of television content. *See also*LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

68 The Electronic Privacy Information Center (EPIC) lists 64 privacy-related bills pending before the U.S. House and Senate, *at*http://www.epic.org/privacy/bill_track.html. In October 2000 a Senate panel held hearings on some proposed privacy legislation. America Online and the Walt Disney Internet Group spoke in favor of "opt-out" legislation sponsored by Senator John McCain. S. 2606, 106th Cong. (2000), *available at*http:// thomas.loc.gov/cgi-bin/bdquery/z?d106:s.02928: Privacy advocacy groups EPIC and the Center for Democracy and Technology spoke in favor of "opt-in" legislation sponsored by Senator Ernest Hollings. S. 2606, 106th Cong. (2000), *available at*http://thomas.loc.gov/cgi-bin/bdquery/z?d106:s.02606:. *See* Jim Wolf, *Opting-out for Online Privacy*, at http://www.abcnews.go.com/sections/tech/DailyNews/onlineprivacy001004.html. Given the current state of public opinion about online privacy, the position of the FTC urging legislation, *supra* note 26, and the sheer number of pending bills, it is only a matter of time before we see some legislation passed.