2. GOVERNANCE BY CONTRACT AND PROMISES

(a) Privacy Policies

Privacy policies are statements made by companies about their practices regarding personal information. Increasingly, companies on the Internet are posting privacy policies, and statutes such as the Gramm-Leach-Bliley Act require certain types of companies (financial institutions, insurance companies, and brokerage companies) to maintain privacy policies.

One of the common provisions of many privacy policies is an "opt-out" provision. An opt-out provision establishes a default rule that the company can use or disclose personal information in the ways it desires so long as the consumer does not indicate otherwise. The consumer must take affirmative steps, such as checking a box, calling the company, or writing a letter, to express her desire to opt out of a particular information use or disclosure. In contrast, an "opt-in" provision establishes a default rule that the company cannot use or disclose personal information without first obtaining the express consent of the individual.

JEFF SOVERN, *OPTING IN, OPTING OUT, OR NO OPTIONS AT ALL: THE FIGHT FOR CONTROL OF PERSONAL INFORMATION*

74 Wash. L. Rev. 1033 (1999)

. . . [F]ew consumers understand how much of their personal information is for sale, although they may have a general idea that there is a trade in personal data and that the specifics about that trade are kept from them. . . .

. . . [C]onsumers cannot protect their personal information when they are unaware of how it is being used by others. . . .

The second reason consumers have not acted to protect their privacy, notwithstanding surveys that suggest considerable consumer concern with confidentiality, has to do with how difficult it is to opt out. . . .

. . . Even if consumers can obtain the information needed to opt out, the cost in time and money of communicating and negotiating with all the relevant information gatherers may be substantial. . . .

Companies may not be eager to offer opt-outs because they may rationally conclude that they will incur costs when consumers opt out, while receiving few offsetting benefits. When consumers exercise the option of having their names deleted, mailing lists shrink and presumably become less valuable. . . .

Because of these added costs, companies might decide that while they must offer an opt-out plan, they do not want consumers to take advantage of it. . . . [C]ompanies that offer opt-outs have an incentive to increase the transaction costs incurred by consumers who opt out. . . .

Companies can increase consumers' transaction costs in opting out in a number of ways. A brochure titled "Privacy Notice," which my local cable company included with its bill, provides an example. This Privacy Notice discussed, among other things, how cable subscribers could write to the company to ask that the company not sell their names and other information to third parties. There are at least four reasons why this particular notice may not be effective in eliciting a response from consumers troubled by the sale of their names to others.

First, the Privacy Notice may be obscured by other information included in the mailing. . . .

The second reason why consumers may not respond to the Privacy Notice is its length. The brochure is four pages long and contains 17 paragraphs, 36 sentences, and 1062 words. . . .

Some companies have gone in the other direction, providing so little information in such vague terms that consumers are unable to discern what they are being told. . . .

A third reason why the Privacy Notice may not be effective stems from its prose. Notwithstanding the Plain Language Law in my home state, computer analysis of the text found it extremely difficult, requiring more than a college education for comprehension. By comparison, a similar analysis of this Article found that it required a lower reading level than that of the Privacy Notice.

Fourth, the Privacy Notice may be ineffective because it does not provide an easy or convenient mechanism for opting out. For example, the Privacy Notice invites consumers who object to the sale of their personal information to write to the cable company in a separate letter. By contrast, cable subscribers desiring to add a new premium channel can do so over the telephone, speaking either to a person or tapping buttons on their telephone, depending on their preference. The more difficult the opt-out process, the less likely consumers are to avail themselves of it. . . .

A third explanation for the failure of consumers to opt out as often as their survey answers might suggest is the consumers themselves. Extensive literature on consumer complaint behavior makes clear that many consumers who are distressed by merchant conduct cannot bring themselves to tell the merchant about it. This inability to communicate might translate into failure by consumers to add their names to opt-out lists. . . .

[Sovern suggests that an opt-in system would be more preferable than an opt-out system.]

One benefit of an opt-in system is that it minimizes transaction costs. While some transaction costs are inevitable in any system in which consumers can opt out or opt in, strategic-behavior transaction costs, at least, can be avoided by using a system which discourages parties from generating such costs. The current system encourages businesses to inflate strategic-behavior costs to increase their own gains, albeit at the expense of consumers and the total surplus from exchange. An opt-in system would encourage businesses to reduce strategic-behavior costs without giving consumers an incentive to increase these costs. Instead of an opt-out situation in which merchants are obligated to provide a message they do not wish consumers to receive, an opt-in regime would harness merchants' efforts in providing a message they want the consumer to receive. . . .

An opt-in system thus increases the likelihood that consumers will choose according to their preferences rather than choosing according to the default. . . .

An opt-in system also increases the prospect that direct mailing would be tailored to what consumers wish to receive, thus benefiting consumers who want to receive some, but not all, solicitations. . . .

The sale of information is troublesome in part because it creates externalities, or costs borne by others. Externalities are created when a person engages in an activity that imposes costs on others but is not required to take those costs into account when deciding whether to pursue the activity. The feelings experienced by consumers whose information is sold and used against their wishes constitute just such externalities. An opt-in system — or an opt-out system in which consumers who object to the trade in their personal information have a genuine opportunity to opt out — can shift costs and thereby "internalize" this externality. To put it another way, consumers could bar the sale of their information unless businesses paid them an amount they deemed adequate, thereby requiring businesses selling personal information to incur a cost otherwise borne by consumers. . . .

A regulated opt-out system is less likely than an opt-in system to solve the problem. Opt-out systems do not give businesses the incentive to minimize consumer transaction costs. Consequently, firms might respond to such regulation by generating formal, legalistic notices that consumers would likely ignore. An opt-out system might thus create only the illusion of a cure.

Accordingly, an opt-in system is preferable, chiefly because it eliminates the incentive firms have to engage in strategic behavior and thus inflate consumer transaction costs. An opt-in system would permit consumers who wish to protect their privacy to do so without incurring transaction costs. Consumers who permit the use of their personal information should also be able to realize their wish easily. Indeed, because firms profit from the use of consumer information, firms would have an incentive to make it as easy as possible for consumers to consent to the use of their personal information. . . . An opt-in system, therefore, seems to offer the best hope of accommodating consumer preferences while minimizing transaction costs. . . .

MICHAEL E. STATEN & FRED H. CATE, *THE IMPACT OF OPT-IN PRIVACY RULES ON RETAIL MARKETS: A CASE STUDY OF MBNA*

52 Duke L.J. 745, 750-51, 766, 770-74, 776 (2003)

To illustrate the costs of moving to an opt-in system, we examine MBNA Corporation, a financial institution that offers consumers a variety of loan and insurance products (primarily credit cards), takes deposits, but operates entirely without a branch network. Incorporated in 1981 and publicly traded since 1991, the company has compiled a stunning growth record in just two decades. As of the end of 2000, the company provided credit cards and other loan products to 51 million consumers, had $89 billion of loans outstanding, and serviced 15 percent of all Visa/MasterCard credit card balances outstanding in the United States.

MBNA's ability to access and use information about potential and existing customers is largely responsible for it becoming the second largest credit card issuer in the United States in less than twenty years. To appreciate the critical role that the sharing of information has played in MBNA's remarkable history, one need only reflect on the challenge of acquiring 51 million customers with no brick-and-mortar stores or branches. Like firms in a variety of businesses, but especially financial services, MBNA harnessed information technology as the engine for establishing and building customer relationships without ever physically meeting its customers. By using direct mail, telephone and, most recently, Internet contacts, the company has reached out to new prospects throughout the population, regardless of where they live, with offers tailored to their individual interests. . . .

At the core of its marketing and targeting strategies is the proposition that consumers who share a common institutional bond or experience will have an affinity for using a card that lets them demonstrate their affiliation each time they use it to pay for a purchase. The affinity for the institution raises the probability that a prospect will be converted to a customer. Equally important, the institution or organization usually maintains a list of members on which MBNA can focus its marketing efforts. Following this "affinity group" marketing strategy, MBNA designs a card product tailored to members of a particular group, negotiates a financial arrangement with the organization for the exclusive rights to market an affinity card to its members, and uses the member list as a source of potential names to contact via direct mail or telemarketing. . . .

Design of new affinity cards is an ongoing process. In 2000 alone, MBNA acquired the endorsements of 459 new groups, including the United States Tennis Association, the Atlanta Braves, National Audubon Society, barnesandnoble.com, and the Thurgood Marshall Scholarship Fund.

Although targeting prospects through affinity groups has proven to be a clever strategy, not every group member is offered a card product. The key to the company's profitability and earnings growth, especially given the rapid growth in the size of the customer base, has been in screening the prospects from each affinity group to identify those likely to be quality customers. Given that MBNA's fundamental business is lending money via an unsecured credit card with a revolving line of credit attached, the company wants to put the card in the hands of customers who will use it, but who will not default on their balances.

Consequently, MBNA uses information to screen prospects both before it makes card offers (the targeting process) and after it receives applications (the underwriting process). . . .

How large a drag does an "explicit-consent" system impose on economic efficiency? According to the U.S. Postal Service, 52 percent of unsolicited mail in this country is never read. If that figure translates to opt-in requests, then more than half of all consumers in an opt-in system would lose the benefits or services that could result from the use of personal information because the mandatory request for consent would never receive their attention. Moreover, even if an unsolicited offer is read, experience with company-specific and industry-wide opt-out lists demonstrates that less than 10 percent of the U.S. population ever opts out of a mailing list — often the figure is less than 3 percent. Indeed, the difficulty (and cost) of obtaining a response of any sort from consumers is the primary drawback of an opt-in approach. . . .

MBNA's core product is the affinity card tailored for and marketed to each of more than 4,700 affinity groups. . . . [T]he foundation of MBNA's affinity strategy is access to the member lists of each of its affinity organizations. This marketing partnership with thousands of member organizations nationwide makes MBNA unique among major credit card issuers and accounts for much of the company's superior financial performance and reputation for outstanding customer service. However, in the absence of an explicit joint-marketing exception in an opt-in law, a third-party opt-in regime could effectively end MBNA's unique direct marketing approach by sharply limiting an organization's ability to share its member list. . . .

Like all major credit card issuers, MBNA uses personal information to increase the chance that its credit card offer will reach an interested and qualified customer. This process greatly reduces the number of solicitations that must be sent to achieve a given target volume of new accounts, thereby reducing the cost of account acquisition. It also reduces the volume of junk mail in the form of card offers sent to consumers who are not qualified. Third-party or affiliate opt-in systems would eliminate MBNA's access to a significant portion of the information that it currently uses to identify which individuals on the member lists it receives would be good prospects for a given credit card or other product. A blanket opt-in system applicable to marketing activities would impose similar limits.

The MBNA direct mail marketing operations obtain and consider about 800 million consumer "leads" during the course of a year. The vast majority of these leads are names that appear on affinity group member lists (e.g., university alumni groups and professional associations), or names of consumers who are customers of institutions that have endorsed MBNA's credit card product. Because this is an annual figure, many names appear more than once because the individuals are on more than one list acquired during the course of a year, or may be considered in conjunction with a specific group's marketing campaign several times during the year. The most creditworthy names among them may receive multiple solicitations during the year.

MBNA does not wish to mail to all names on the list. Not all are equally likely to respond to a solicitation, nor will all meet the credit underwriting standards for a particular card product. In 2000, the MBNA direct marketing

budget supported approximately 400 million mailings of card offers. The challenge to the company in managing the acquisition of new accounts is to cull the "lead list" of 800 million prospect names to identify and target the 400 million direct mail solicitations to consumers who are most likely to become new cardholders. Generally speaking, MBNA has developed a set of targeting criteria such that names reaching the final mailing list of 400 million: (1) are most likely to respond to the offer and the use of the credit card, and (2) are most likely to meet MBNA's creditworthiness standards for the card.

MBNA prepares hundreds of distinct solicitations throughout the year for its various affinity groups. As part of the targeting process for each new solicitation, the prospect list is scrubbed via comparison to a series of "suppression files" that the company maintains and routinely updates. These files pull information about either individuals or addresses from a variety of internal and external data sources. A few examples of the specific criteria illustrate the process.

[The authors describe how MBNA has proprietary response models to help it determine which customers are most likely to respond to its offer. It uses credit history information to find individuals who are likely to repay, but, at the same time, do not have "extraordinary creditworthiness" and are, hence, likely to be frequently solicited by card issuers and unlikely to respond to an MBNA offer.]

The bottom line from the culling process is that approximately 40 percent of the eight hundred million names are suppressed. The initial lead list is typically reduced by an additional 10 percent through a combination of eliminating duplicate records, suppressing undeliverable addresses, and dropping customer names that appear on various "do not mail" lists that record customer preferences not to be solicited. . . . The approximately four hundred million names remaining on the lead list receive targeted direct mail offers with the endorsement of the affinity group to which they belong. . . .

MBNA's proprietary response models indicate that its use of information in these three categories to cull likely prospects accounts for approximately a 19 percent reduction in names from the annual prospect list. In other words, by targeting offers under current rules, about 150 million names on the prospect list during the course of a typical annual solicitation cycle do not receive solicitations, because the direct mail piece would otherwise reach a consumer who was either not interested or not qualified for the card product. . . .

[Under an opt-in approach,] approximately 550 million names would remain, instead of 400 million under the current rules. Lacking the information necessary to further distinguish good prospects from poor prospects, the company's targeting efficiency would be impaired.

MBNA would have two choices. It could increase its direct mail volume to send solicitations to all 550 million names remaining on the prospect list after the culling process, or it could arbitrarily remove 150 million names from the list after the culling process so that its direct mail volume remained unchanged at 400 million. Under either scenario, approximately 27 percent of the solicitations (150 million of 550 million) would go to consumers who were less interested in, and/or less qualified for, the offer, and who would have been dropped from the target list had MBNA been allowed to access and use the information on which its presently relies under current privacy rules. . . .

Although MBNA's actual response rate and cost per account booked is proprietary, we can illustrate the impact of the decline by utilizing the credit card industry average response rate to direct mail solicitations for 2000, which was 0.6 percent. For every 100 million solicitations mailed to individuals under the opt-in scenario, only 492 thousand new accounts would be booked, as compared to 600 thousand if the offers were targeted under existing rules, an 18 percent reduction in new accounts for the same expenditure on direct mail solicitations. Of course, the higher cost per account booked is borne not only by MBNA, but by MBNA's customers as well, in the form of higher prices, reduced benefits, diminished service, and higher acceptance standards for new credit products.

But, the negative impact does not stop there. Regardless of whether MBNA's response to opt-in is to mail more solicitations or mail the same number to a less-targeted prospect list, under either scenario, the recipient group of four hundred million individuals will — on average — be more risky and less profitable than MBNA's target group reached under the current rules. As a result, MBNA's delinquency and charge-off rates will rise, relative to its current experience, thereby imposing additional costs that will be passed along to all of MBNA's customers. Card usage will also be affected by booking cardholders who are less likely to use the card.

NOTES & QUESTIONS

1. ***Opt out vs. Opt in.*** Do you agree with Sovern that an opt-in policy is more efficient than an opt-out policy? Do you think that an opt-in policy is feasible? Are the views of Staten and Cate convincing on this score? Do you think opt out or opt in should be required by law?
2. ***Internalizing Costs.*** Staten and Cate claim that MBNA's business model will be threatened by opt in. This business model relies in part, however, on sending out 400 million of mostly unwanted solicitations for credit in order to receive a 0.6 percent response rate. In other words, this model views as an externality the added cost of sorting through mail for 99.4 percent of those individuals solicited. Should MBNA be obliged to internalize these costs?

Enforcing Privacy Policies as Contracts AGAINST Consumers:

Allyson Haynes: [T]here is a distinct possibility that as website operators grow savvier with respect to the law, they will respond to the lack of substantive privacy protection (and lack of consumer awareness) by including in privacy policies terms that are not favorable to consumers.

On the flip side of consumers seeking to enforce privacy policies as contracts, companies might also desire to hold customers to be contractually bound to the companies' privacy policies. Would a privacy policy be enforceable as a contract against the customer? Haynes contends:

> [P]articularly in cases where consumers are deemed to have assented to privacy policies by virtue of their presence on the site or by giving information without affirmatively clicking acceptance, the consumer has a good argument that he or she did not assent to the privacy policy, preventing the formation of a binding contract, and preventing the website from enforcing any of its terms against the consumer.[30]

(c) FTC Enforcement

Beyond private law actions such as contract and promissory estoppel, the promises that companies make regarding their privacy practices can be enforced by the government through public law. Private law actions are initiated on behalf of harmed individuals, who can obtain monetary or other redress for their injuries. In contrast, public law actions are initiated by government agencies or officials, and they typically involve fines and penalties.

In 1995, Congress and privacy experts first asked the Federal Trade Commission (FTC) to become involved with consumer privacy issues.[31] Since 1998, the FTC has maintained the position that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act, 15 U.S.C. § 45. The Act prohibits "unfair or deceptive acts or practices in or affecting commerce." An "unfair or deceptive" act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." § 45(n).

The FTC does not have jurisdiction over all companies. Exempt from the FTC's jurisdiction are many types of financial institutions, airlines, telecommunications carriers, and other types of entities. § 45(a)(2). The Act authorizes the FTC to bring civil actions for penalties up to $10,000 for a knowing violation of the Act. § 45(m)(1)(A). Further, the FTC can obtain injunctive remedies. § 53. The Act does not provide for private causes of action; only the FTC can enforce the Act. Since it began enforcing the Act for breaches of privacy policies in 1998, the FTC has brought a number of actions, most of which have settled. Some of these enforcement cases concern companies not

---

[30] Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 Penn. St. L. Rev. 587, 612, 618 (2007).

[31] Letter from EPIC Director Marc Rotenberg to FTC Commissioner Christine Varney, Dec. 14, 1995.

keeping their privacy promises. As a more complicated example of a violation of the FTC Act, consider *In the Matter of Vision I Properties*.

IN THE MATTER OF VISION I PROPERTIES

2005 WL 1274741 (F.T.C. 2005)

[Vision I Properties licensed shopping cart software and provided related services to small online retail merchants through a website, www.cartmanager.com. The company's software created customizable shopping cart pages for client merchants' websites. The resulting pages resided on websites managed by Vision I Properties, but resembled the other pages on merchants' websites.

Some of the client merchants using this company's shopping cart software and services published various privacy policies on their websites. In its complaint, the FTC excerpted some of these privacy policies, including one that stated: "PRIVACY POLICY: It's simple. We don't sell, trade, or lend any information on our customers or visitors to anyone."

In fact, however, Vision I Properties in January 2003 rented consumers' personal information collected through its shopping cart and check out pages at client merchant sites. The FTC complaint noted: "Such personal information includes the name, address, phone number, and purchase history of nearly one million consumers. This personal information was used by third parties to send direct mail and make telemarketing calls to consumers who shopped at merchant sites using the software."

For the FTC, it was reasonable for consumers to rely on merchants' privacy policies. Moreover, Vision I Properties did not adequately inform merchants of its information sharing. It did assert, however, in its online license agreement that it would retain "full ownership of all data submitted by either Merchant or Purchaser." The FTC dismissed this statement, however, as (1) "buried in the middle of the online agreement" and also as (2) lacking an explanation of how Vision I Properties intended "to use the information or that such use may conflict with the merchants' privacy policies."

On April 19, 2005, the FTC and Vision I properties settled the case and the FTC issued a Decision and Order.]

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act. . . .

I.

IT IS ORDERED that Respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the collection of personally identifiable information from or about consumers, shall not make, expressly or by implication, any false or misleading representation regarding the collection, use, or disclosure of personally identifiable information.

II.

IT IS FURTHER ORDERED that Respondent, directly or through any corporation, subsidiary, division, or other device, shall not sell, rent, or disclose to any third party for marketing purposes any personally identifiable information that was collected from consumers through shopping cart software used at a merchant customer's Web site prior to the date of service of this Order.

III.

IT IS FURTHER ORDERED that Respondent, directly or through any corporation, subsidiary, division, or other device, shall not sell, rent, or disclose to any third party for marketing purposes any personally identifiable information collected from consumers through shopping cart or other software used at a merchant customer's Web site after the date of service of this Order unless, prior to the date such information was collected, Respondent took one of the following two actions:

A. Provided to the merchant customer a clear and conspicuous written notice of its information practices and obtained from the merchant customer a written certification stating: (1) that the merchant customer received such notice; and (2) either (a) that its posted privacy policy states that consumers' information may be sold, rented, or disclosed to third parties, or (b) that it provides a clear and conspicuous disclosure, before any personally identifiable information is collected from consumers through Respondent's shopping cart or other software, stating that the consumer is leaving the merchant customer's Web site and entering Respondent's Web site, and that Respondent's site is governed by Respondent's own privacy policy.

The written notice to merchants required by this Paragraph shall be labeled "Important Notice to Merchants from CartManager" and must: (1) state that Respondent intends to sell, rent, or disclose such information; (2) identify the types or categories of any entities to which such information will be disclosed; (3) advise the merchant customer that it may be liable for any misrepresentations it makes about the use or disclosure of information collected from consumers at its Web site, including through software used at the site; and (4) contain no other information; OR

B. Provided a clear and conspicuous disclosure on the page(s) through which it collected such information stating: (1) that the consumer is on Respondent's Web site, and (2) that information provided by the consumer to Respondent will be used, sold, rented, or disclosed to third parties for marketing purposes.

IV.

IT IS FURTHER ORDERED that within five (5) days of the date of service of this Order, Respondent shall pay $9,101.63 to the United States Treasury as disgorgement. Such payment shall be by cashier's check or certified check made payable to the Treasurer of the United States. In the event of any default in payment, which default continues for more than ten (10) days beyond the due date of payment, Respondent shall also pay interest as computed under 28 U.S.C. § 1961, which shall accrue on the unpaid balance from the date of default until the date the balance is fully paid.

V.

IT IS FURTHER ORDERED that Respondent Vision One and its successors and assigns shall, for a period of five (5) years after the last date of dissemination of any representation covered by this Order, maintain and upon request make available to the Federal Trade Commission for inspection and copying a print or electronic copy of all documents demonstrating their compliance with the terms and provisions of this Order, including, but not limited to:

A. A sample copy of each different privacy statement or communication relating to the collection of personally identifiable information containing representations about how personally identifiable information will be used and/or disclosed. Each Web page copy shall be dated and contain the full URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting the information on the Web; *provided, however*, that after creation of any Web page or screen in compliance with this Order, Respondent shall not be required to retain a print or electronic copy of any amended Web page or screen to the extent that the amendment does not affect Respondent's compliance obligations under this Order;

B. A sample copy of each different document containing the disclosures required by Part III.A. of this Order; a list of all merchant customers who received each different document containing such disclosures; all communications by merchant customers in response to such disclosures, including all written certifications received pursuant to Part III.A. and any complaints received from merchant customers; and a sample copy of each different document containing the disclosures required by Part III.B.; and

C. All invoices, communications, and records relating to the disclosure to third parties of personally identifiable information collected through merchant customer Web sites. . . .

VII.

IT IS FURTHER ORDERED that Respondent Vision One and its successors and assigns shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this Order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the

creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. . . .

IX.

This Order will terminate on April 19, 2025, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the Order, whichever comes later. . . .

NOTES & QUESTIONS

1. ***Responsibility for Violating Another Company's Privacy Policy?*** In a typical "broken promise" privacy case, the FTC charges a company with breaking its own promise to provide certain kinds of privacy practices or protections. In contrast, the FTC in *Vision I Properties* was faced with a situation in which the behavior of Vision I broke the privacy promises of other parties (the merchants). Vision I Properties does not seem to be in privity with the end customers; it is a B2B (business-to-business) company rather than a B2C (business-to-consumer) company.

   To be sure, Vision I Properties prevented its merchant customers from delivering on their privacy policies. Yet, Vision I Properties had a provision in its contracts with the merchants explicitly claiming ownership of all information collected with use of its software. By pursuing an action against Vision I Properties, the FTC was claiming that its behavior was an unfair or deceptive trade practice. But if a merchant has a privacy policy, why isn't the burden on the merchant to police the behavior of the B2B entities with whom it contracts? Shouldn't the merchants be liable for lack of care in reading their contracts?
2. ***Damages.*** *In the Matter of Vision I Properties,* the FTC assesses damages of $9,101.63 "as disgorgement." A disgorgement measure of damages looks to the unjust enrichment of a defendant and requires her to surrender a profit improperly or illegally obtained. Is the proper measure of damages in this case the disgorgement of profits that Vision I Properties obtained through its practices in renting the information it collected through its shopping cart software?
3. ***Broken Promises:*** **Liberty Financial.** In *In re Liberty Financial Cos.,* No. 9823522, 1999 FTC LEXIS 99 (May 6, 1999), the FTC charged the operator of a website for child and teen investors with falsely promising that the personal information it collected in a survey would be kept anonymous. The website gathered data about the child and family's finances, but instead of being anonymously maintained, it was kept in an identifiable form. Liberty Financial settled with the FTC, agreeing to refrain from making future misrepresentations, to post a privacy notice on its website, and to obtain

parental consent prior to gathering personal data from children. FTC commissioners approved the settlement 4–0.

4. ***Deceptive Data Collection:*** **ReverseAuction.** In *FTC v. ReverseAuction.com, Inc.*, No. 00-CV-32 (D.D.C. Jan. 6, 2000), the FTC charged ReverseAuction.com with improperly obtaining personal information from eBay customers. ReverseAuction then used the information to spam eBay customers promoting its own auction website. The message falsely stated to the recipients that their eBay user IDs would expire soon. The FTC charged that ReverseAuction's practice was both unfair and deceptive.

ReverseAuction settled, agreeing to be barred from making future misrepresentations. Further, ReverseAuction had to notify the consumers who received its spam and inform them that its eBay user IDs will not expire and that eBay did not authorize ReverseAuction's spam. Consumers also can delete their personal information from ReverseAuction's database. ReverseAuction must also display its own privacy policy on its website. FTC commissioners voted 5–0 to approve the settlement. However, two commissioners, Orson Swindle and Thomas B. Leary, agreeing that ReverseAuction acted deceptively, disagreed that ReverseAuction acted unfairly:

> We do not, however, support the unfairness theory in Count One. The Commission has no authority to declare an act or practice unfair unless it "causes or is likely to cause *substantial injury* to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (emphasis added). . . .
>
> We do not say that privacy concerns can never support an unfairness claim. In this case, however, ReverseAuction's use of eBay members' information to send them e-mail did not cause substantial enough injury to meet the statutory standard. . . .
>
> The injury in this case was caused by deception: that is, by ReverseAuction's failure to honor its express commitments. It is not necessary or appropriate to plead a less precise theory.
>
> . . . The unfairness theory . . . posits substantial injury stemming from ReverseAuction's use of information readily available to millions of eBay members to send commercial e-mail. This standard for substantial injury overstates the appropriate level of government-enforced privacy protection on the Internet, and provides no rationale for when unsolicited commercial e-mail is unfair and when it is not.

One commissioner, Mozelle W. Thompson, issued a separate statement to justify the unfairness theory:

> I believe that ReverseAuction's behavior caused substantial injury to members of the eBay community, that the injury could not have been avoided by those members, and it was not outweighed by countervailing benefits. I believe the harm caused in this case is especially significant because it not only breached the privacy expectation of each and every eBay member, it also undermined consumer confidence in eBay and diminishes the electronic marketplace for all its participants. This injury is exacerbated because consumer concern about

privacy and confidence in the electronic marketplace are such critical issues at this time.

5. ***Retroactive Privacy Policy Changes:*** **Gateway Learning Corp.** When Gateway Learning Corp. collected personal information from its consumers, its privacy policy stated that it would not sell, rent, or loan personal information to third parties unless people consented. Subsequently, Gateway altered its privacy policy to allow the renting of personal information to third parties without informing customers or obtaining their consent. The FTC filed a complaint alleging that this practice was an "unfair" act. *See In re Gateway Learning Corp.*, No. C-4120 (Sept. 10, 2004). Gateway settled with the FTC, agreeing to avoid making deceptive claims or retroactively change its privacy policy without consumer consent. Gateway agreed to pay $4,608, the amount it earned from renting the information.

   Suppose a company puts the following line in its privacy policy: "Please be aware that we may change this policy at any time." Would this allow for the retroactive application of a revised policy? Or is there an argument that even with a statement such as this one, the revised policy could not be applied retroactively?

6. ***Privacy Promises and Bankruptcy:*** **Toysmart *and Amazon.com.*** In *FTC v. Toysmart.com, LLC*, Civ. Action No. 00-11341-RGS (July 21, 2000), an Internet toy retailer, Toysmart.com, went bankrupt in 2000. One of the company's most important assets was its database of personal information — it had a customer list with over 200,000 individual names. This list included addresses, names and ages of children, purchasing information, and a toy wish list. Toysmart was a member of TRUSTe, an e-commerce industry privacy protection organization that establishes rules for privacy policies and permits companies that follow them to display TRUSTe's privacy seal. Toysmart had agreed to follow TRUSTe's guidelines and had displayed the TRUSTe seal on its website.

   In its privacy policy, Toysmart promised: "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." To pay back creditors, Toysmart attempted to sell its database of personal information.

   The FTC filed a complaint objecting to this practice and argued that such a sale, in light of Toysmart's promises never to sell its customer's personal information, would be a deceptive practice. The FTC approved a settlement by a 3–2 vote restricting how Toysmart could sell its database. The settlement states that:

   > The Debtor shall only assign or sell its Customer Information as part of the sale of its Goodwill and only to a Qualified Buyer approved by the Bankruptcy Court. In the process of approving any sale of the Customer Information, the Bankruptcy Court shall require that the Qualified Buyer agree to and comply with the terms of this Stipulation.

> The Qualified Buyer shall treat Customer Information in accordance with the terms of the Privacy Statement and shall be responsible for any violation by it following the date of purchase. Among other things, the Qualified Buyer shall use Customer Information only to fulfill customer orders and to personalize customers' experience on the Web site, and shall not disclose, sell or transfer Customer Information to any Third Party.
>
> If the Qualified Buyer materially changes the Privacy Statement, prior notice will be posted on the Web site. Any such material change in policy shall apply only to information collected following the change in policy. The Customer Information shall be governed by the Privacy Statement, unless the consumer provides affirmative consent ("opt-in") to the previously collected information being governed by the new policy. . . .

Is this settlement adequate to resolve the problems raised by the FTC in its complaint? As a postscript, one should note that the settlement attracted the support of Toysmart's creditors, since it would allow the sale of the database to certain purchasers, and hence could be used to pay back the creditors. However, in August 2000, Judge Carol Kenner of the U.S. Bankruptcy Court rejected the settlement because there were currently no offers on the table to buy the database, and it would hurt the creditors to restrict the sale to certain types of purchasers without first having a potential buyer. In February 2001, Judge Kenner agreed to let Toysmart sell its customer database to Disney, the primary shareholder, for $50,000. Disney agreed, as part of the deal, to destroy the list.

The Toysmart bankruptcy also led Amazon.com, the Internet's largest retailer, to change its privacy policy. Prior to the Toysmart case, Amazon's privacy policy provided:

> Amazon.com does not sell, trade, or rent your personal information to others. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com.

In its new policy, Amazon.com stated:

> Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only with the subsidiaries Amazon.com, Inc., controls and as described below. . . .
>
> 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. . . .

Amazon.com's new policy was criticized by some privacy organizations. One of the criticisms was that the policy did not provide an opt-out right. Suppose Amazon.com went bankrupt and decided to sell all of its customer data. Can it sell data supplied by consumers under the old policy? Can the new policy apply retroactively?

7. ***Bankruptcy: Property Rights vs. Contract Rights.*** Edward Janger proposes that a property rights regime (as opposed to the contractual rights of a privacy

policy) will best protect the privacy of personal data when companies possessing such data go bankrupt:

> Property rules are viewed as reflecting undivided entitlements. They allocate, as Carol Rose puts it, the "whole meatball" to the "owner." Liability rules, by contrast are viewed as dividing an entitlement between two parties. One party holds the right, but the other party is given the option to take the right and compensate the right holder for the deprivation (to breach and pay damages). . . .
>
> Propertization has some crucial benefits, but it also has some serious costs. Both the bankruptcy and non-bankruptcy treatment of privacy policies turn on whether a privacy policy creates a right enforceable only through civil damages, or a right with the status of property. If bankruptcy courts treat privacy policies solely as contract obligations [liability rule], the debtor will be free to breach (or reject) the contract in bankruptcy. Any damage claim will be treated as a prepetition claim, paid, if at all, at a significant discount. Consumer expectations (contractual or otherwise) of privacy are likely to be defeated. By contrast, if personal information is deemed property subject to an encumbrance, then the property interest must be respected, or to use the bankruptcy term, "adequately protected."

In other words, Janger contends that giving individuals property rights in their personal data will provide more protection than giving individuals contract rights in the event a company goes bankrupt. Janger further argues that property rights alone will not be sufficient. Property rights must be "muddy" rather than "crystalline":

> . . . A crystalline rule places all of the relevant rights firmly in the hand of the entitlement holder or "owner." A muddier standard leaves the right subject to challenge by a competing claimant. Crystalline rules situate decisionmaking and norm-generating authority in either the legislature or the market. Muddy rules lead to decisions made and legal norms articulated by judges. . . .
>
> . . . [M]uddy standards force parties ex ante to recognize that they might have to justify their contractual terms and negotiating behavior ex post. This attribute of muddy rules operates to enforce behavioral norms in ways that crystalline rules do not. Efforts to resolve norm-based disputes force disclosure of information related to the norm. This norm-based information forcing effect has both public and private implications. Muddy rules may improve the contracting behavior of parties, but muddy rules also serve a more public purpose. Muddy rules force information into the legal system about transactions. They allow judges, and the judiciary, to develop rules incrementally, through common law reasoning, and inform legislative decisionmaking by placing disputes on the record. But muddiness alone is not enough. The benefits of the muddy liability rule may evaporate entirely when a debtor goes bankrupt. These behavior regulating and information forcing effects of muddy rules are maximized only when the muddy rule is given the status of property.[32]

---

[32] Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 Wm. & Mary L. Rev. 1801 (2002).

8. ***Customer Databases as Collateral.*** Xuan-Thao Nguyen points out that companies are using their customer databases as collateral for loans, since these databases are one of their most significant assets:

> Whether intentional or unintentional, many Internet companies ignore their own privacy policy statements when the companies pledge their customer database as collateral in secured financing schemes. This practice renders online privacy statements misleading because the statements are silent on collateralization of the company's assets. . . .
>
> The secured party can use the consumer database in its business or sell the consumer database to others. The collateralization of the consumer database and its end result may contradict the debtor's consumer privacy statement declaring that the debtor does not sell or lease the consumer information to others. Though there is no direct sale of the consumer database to the secured party, the effect of the collateralization of the consumer database is the same: the consumer database is in the hands of third parties with unfettered control and rights. Essentially, the collateralization of consumer databases violates the privacy policies publicized on debtors' Web sites.[33]

9. ***The FTC as an Enforcer of Privacy: An Assessment.*** In 2000, Steven Hetcher assessed the FTC's behavior in enforcing privacy in these terms:

> By the Agency's lights, its promotion of the fair practice principles should satisfy privacy advocates, as the fair information practice principles are derived from pre-existing norms of the advocacy community. Public interest advocates contend to the contrary, however, that privacy policies ill serve their aspirational privacy norms. They argue that privacy policies are typically not read by website users. They are written in legalese such that even if people read them, they will not understand them. Hence, they do not provide notice and thus cannot lead to consent. In addition, there is evidence that many sites do not adhere to their own policies. The policies are subject to change when companies merge, such that one company's policy is likely to go unheeded. Finally, very few privacy policies guarantee security or enforcement. Thus, the provision of a privacy policy by a website does not automatically promote the fair practice principles.
>
> Despite these problems, the FTC has strongly endorsed privacy policies. This raises a puzzle as to why the Agency should do so, given the severe criticism privacy policies have received. Why, for instance, is the FTC not coming out in support of the creation of a new agency to oversee privacy protection? . . .
>
> There is a public choice answer as to why the Agency has promoted privacy policies, despite their problems (and despite the fact that they do not appear to promote the interests of any industry groups whose favor the FTC might be seeking). It is through privacy policies that the FTC is gaining jurisdiction over the commercial Internet. Jurisdiction is power. In other words, the FTC acts as if it has a plan to migrate its activities to the Internet, and privacy policies have been at the core of this plan. . . .[34]

---

[33] Xuan-Thao N. Nguyen, *Collateralizing Privacy*, 78 Tul. L. Rev. 553, 571, 590 (2004).

[34] Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 Vand. L. Rev. 2041 (2000). *See also* Steven Hetcher, *Norms in a Wired World* (2004); Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 Harv. J. L. & Tech. 149 (2001); Steven A. Hetcher,

Joel Reidenberg argues that the FTC is the wrong choice to regulate privacy in the United States:

> Public enforcement of data privacy relies on an expedient set of actors who are generally mismatched to remedy public wrongs. The public actors do not have specific statutory privacy rights authority. Instead, they exploit derivative powers to play a role in privacy claims. At the federal level, the current enforcement agency is the Federal Trade Commission. In many ways, this agency is an illogical choice for the protection of citizens' privacy. The FTC's mission is to enforce antitrust and certain consumer protection laws:
>
> > The Commission seeks to ensure that the nation's markets function competitively, and are vigorous, efficient, and free of undue restrictions. The Commission also works to enhance the smooth operation of the marketplace by eliminating acts or practices that are unfair or deceptive.
>
> Reliance on the FTC as a primary enforcer of citizen privacy is misplaced. The prevention of privacy wrongs, and particularly the public wrongs, as such, is simply not part of the core mission of the FTC. The FTC is not charged with the enforcement of civil rights, nor is the agency equipped or permitted to handle employment or telecommunications privacy matters. In fact, the FTC only grudgingly accepted involvement with privacy issues. During the mid-1990s, Commissioner Christine Varney persistently raised privacy as an important issue. For many years, the FTC hoped that the market would self-regulate and did not want to intervene aggressively. The FTC even opposed new federal legislation to protect information privacy. . . .
>
> While the FTC seems to be the federal regulator of choice for a light touch in enforcement against privacy wrongs, the states' Attorneys General have taken a more aggressive stance. The National Association of Attorneys General has an Internet Law task force that studies and coordinates the enforcement of privacy. In effect, the states are unwilling to wait for federal results. This more aggressive stance of public enforcement at the state level is illustrated well by an enforcement action brought against DoubleClick. In February 2000, the Electronic Privacy Information Center ("EPIC"), a prominent privacy advocacy group, filed a complaint against DoubleClick with the Federal Trade Commission based on the company's practice of profiling web users without adequate disclosure. EPIC's complaint focused on the lack of disclosure and on profiling as an "unfair and deceptive practice." The FTC eventually closed its investigation with no action. However, a coalition of ten states pursued DoubleClick's practices and compelled DoubleClick to accept a binding agreement regarding privacy policies and disclosure; DoubleClick also accepted a fine of $450,000 to reimburse the states' investigative costs.
>
> Like the federal actions, the state cases that rely on "unfair and deceptive practices" statutory authority do not address the public wrongs directly. When states pursue claims, the results are only able to achieve company specific cessations of particular data processing practices. These remedies address specific harms to individuals rather than the broader harms caused by widespread practices.[35]

Norm Proselytizers Create a Privacy Entitlement in Cyberspace, 16 Berkeley Tech. L.J. 877 (2001).

[35] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L.J. 877 (2003).

After these writings by Hetcher and Reidenberg, however, the FTC developed an additional role — the agency began to enforce standards of data security. Does this role fit in with Hetcher's analysis ("through privacy policies . . . the FTC is gaining jurisdiction over the commercial Internet") or Reidenberg's ("the FTC seems to be the federal regulator of choice for a light touch in enforcement")?

10. ***State Deceptive Trade Practices Acts.*** In addition to the FTC Act, which is enforced exclusively by the FTC, every state has some form of deceptive trade practices act of its own. Many of these statutes not only enable a state attorney general to bring actions but also provide a private cause of action to consumers. Several of these laws have provisions for statutory minimum damages, punitive damages, and attorneys' fees. *See, e.g.*, Cal. Civ. Code § 1780(a)(4) (punitive damages); Conn. Gen. Stat. § 42-110g(a) (punitive damages); Mich. Comp. Laws § 445.911(2) (minimum damages); N.Y. Gen. Bus. Law § 349(h) (minimum damages). In interpreting these state laws, many state courts have been heavily influenced by FTC Act jurisprudence. However, as Jeff Sovern notes, many states "have been more generous to consumers than has the FTC," and "even if the FTC concludes that practices pass muster under the FTC Act, it is still at least theoretically possible for a state to find the practices deceptive under their own legislation." Thus, Sovern concludes, "information practices that are currently in widespread use may indeed violate state little FTC Acts. Marketers should think carefully about whether they wish to alter their practices."[36]

3. GOVERNANCE BY SELF-REGULATION

Pure Self-Regulation. Some commentators contend that the best solution to data collection and use is to allow companies to regulate themselves. Fred Cate points out that self-regulation is "more flexible and more sensitive to specific contexts and therefore allow[s] individuals to determine a more tailored balance between information uses and privacy than privacy laws do."[37]

Eric Goldman argues:

> Relatively few consumers have bought privacy management tools, such as software to browse anonymously and manage Internet cookies and e-mail. Many vendors are now migrating away from consumer-centric business models. So, although consumers can take technological control over their own situation, few consumers do.
>
> Plus, as most online marketers know, people will "sell" their personal data incredibly cheaply. As Internet pundit Esther Dyson has said: "You do a survey, and consumers say they are very concerned about their privacy. Then you offer them a discount on a book, and they'll tell you everything." Indeed, a recent Jupiter report said that 82% of respondents would give personal information to new shopping sites to enter a $100 sweepstakes.

---

[36] Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 Fordham L. Rev. 1305, 1352-53, 1357 (2001).

[37] Fred H. Cate, *Privacy in Perspective* 26 (2001); *see also* Fred H. Cate, *Privacy in the Information Age* (1997).

> Clearly consumers' stated privacy concerns diverge from what consumers do. Two theories might explain the divergence.
>
> First, asking consumers what they care about reveals only whether they value privacy. That's half the equation. Of more interest is how much consumers will pay — in time or money — for the corresponding benefits. For now the cost-benefit ratio is tilted too high for consumers to spend much time or money on privacy.
>
> Second, consumers don't have uniform interests. Regarding online privacy, consumers can be segmented into two groups: activists, who actively protect their online privacy, and apathetics, who do little or nothing to protect themselves. The activists are very vocal but appear to be a tiny market segment.
>
> Using consumer segmentation, the analytical defect of broad-based online privacy regulations becomes apparent. The activists, by definition, take care of themselves. They demand privacy protections from businesses and, if they don't get it, use technology to protect themselves or take their business elsewhere.
>
> In contrast, mainstream consumers don't change their behavior based on online privacy concerns. If these people won't take even minimal steps to protect themselves, why should government regulation do it for them?
>
> Further, online businesses will invest in privacy when it's profitable. . . . When companies believed that few consumers would change their behavior if they were offered greater privacy, those companies did nothing or put into place privacy policies that disabused consumers of privacy expectations. Of course, if companies later discovered that they were losing business because customers wanted more privacy, they would increase their privacy initiatives.
>
> Consumer behavior will tell companies what level of privacy to provide. Let the market continue unimpeded rather than chase phantom consumer fears through unnecessary regulation.[38]

In contrast, Peter Swire contends that privacy legislation need not be antithetical to business interests. According to Swire, privacy legislation should be viewed as similar to the "trustwrap" that Johnson & Johnson placed around bottles of Tylenol after a scare involving cyanide poisoning of the pain reliever.[39] Swire believes that "privacy legislation targeted at online practices" would provide the kind of safety to allow consumers to engage in cyberspace activities with confidence.

Default Rules. In contrast to a pure self-regulatory approach, in which personal information belongs to whatever entity happens to obtain it, Jerry Kang argues that a default rule that individuals retain control over information they surrender during Internet transactions is more efficient than a default rule where companies can use the data as they see fit. According to Kang, the latter default rule would create two inefficiencies for individuals in attempting to bargain around the rule:

> . . . First, [the individual] would face substantial research costs to determine what information is being collected and how it is being used. That is because individuals today are largely clueless about how personal information is

---

[38] Eric Goldman, *The Privacy Hoax*, Forbes (Oct. 14, 2002), available at http://www.ericgoldman.org/Articles/privacyhoax.htm.

[39] Peter P. Swire, *Trustwrap: the Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 Hastings L.J. 847 (2003).

> processed through cyberspace. Transacting parties and transaction facilitators do not generally provide adequate, relevant notice about what information will be collected and how it will be used. What is worse, consumer ignorance is sometimes fostered by deceptive practices.
>
> Second, the individual would run into a collective action problem. Realistically, the information collector — the "firm" — would not entertain one person's idiosyncratic request to purchase back personal information because the costs of administering such an individually tailored program would be prohibitive. This explains the popular use of form contracts, even in cyberspace, that cannot be varied much, if at all. Therefore, to make it worth the firm's while, the individual would have to band together with like-minded individuals to renegotiate the privacy terms of the underlying transaction. These individuals would suffer the collective action costs of locating each other, coming to some mutual agreement and strategy, proposing an offer to the information collector and negotiating with it — all the while discouraging free riders. . . .

Therefore, Kang argues, the appropriate default is to give control of information to the individual:

> With this default, if the firm valued personal data more than the individual, then the firm would have to buy permission to process the data in functionally unnecessary ways. Note, however, two critical differences in contracting around this default. First, unlike the individual who had to find out what information is being collected and how it is being used, the collector need not bear such research costs since it already knows what its information practices are. Second, the collector does not confront collective action problems. It need not seek out other like-minded firms and reach consensus before coming to the individual with a request. This is because an individual would gladly entertain an individualized, even idiosyncratic, offer to purchase personal information. In addition, there will be no general "holdout" problem because one individual's refusal to sell personal information to the collector will not generally destroy the value of personal information purchased from others.[40]

Would Kang's approach serve as a dramatic change for the self-regulatory approach? Couldn't companies regularly bargain around Kang's default rule in order to obtain control of the data from individuals? Does assigning the initial entitlement make a practical difference?

Flexible Regulation. Some commentators contend that a middle ground can be found between traditional legal regulation and self-regulation. Dennis Hirsch argues that environmental law suggests ways to regulate privacy that are flexible and that mix legal regulation with self-regulation:

> Over the past forty years, environmental law has been at the epicenter of an intense and productive debate about the most effective way to regulate. Initial environmental laws took the form of prescriptive, uniform standards that have come to be known as "command-and-control" regulation. These methods, while effective in some settings, proved costly and controversial. In the decades that followed, governments, academics, environmental and business groups, and others poured tremendous resources into figuring out how to improve upon these

[40] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193, 1253-54, 1257 (1998).

> methods. This work has produced a "second generation" of environmental regulation. . . .
>
> Second generation initiatives encourage the regulated parties themselves to choose the means by which they will achieve environmental performance goals. That is what defines them and distinguishes them from first generation regulations under which the agency has the primary decisionmaking power over pollution control methods. This difference tends to make second generation strategies more cost-effective and adaptable than command-and-control rules. The proliferation of second generation strategies has led some to identify the environmental field as having "some of the most innovative regulatory instruments in all of American law."
>
> Privacy regulation today finds itself in a debate similar to the one that the environmental field has been engaged in for years. On the one hand, there is a growing sense that the digital age is causing unprecedented damage to privacy and that action must be taken immediately to mitigate these injuries. On the other, a chorus of voices warns against the dangers of imposing intrusive and costly regulation on the emerging business sectors of the information economy. Missing thus far from the dialogue is any significant discussion of the more flexible "second generation" regulatory strategies that might be able to bridge this gap. It took environmental law decades to arrive at these alternatives. The privacy field could capitalize on this experience by looking to these environmental policies as models for privacy regulation.[41]

Is the analogy of privacy law to environmental law an apt one? To what extent are the privacy statutes discussed in this book thus far command-and-control rules versus flexible rules? Is Hirsch calling less for self-regulation than for industry input into the form and content of rules?

Regulation by Technology. As part of the self-governance, technology can assist companies as well as consumers in making privacy choices. Privacy on the Internet can be protected by another form of regulatory mechanism — technology. According to Joel Reidenberg, "law and government regulation are not the only source of rule-making. Technological capabilities and system design choices impose rules on participants."[42] Reidenberg calls such forms of technological governance "Lex Informatica."

In the privacy context, Privacy Enhancing Technologies (PETs) have received much attention from scholars and the privacy policy community. Herbert Burkert describes PETs as "technical and organizational concepts that aim at protecting personal identity. These concepts usually involve encryption in the form digital signatures, blind signature or digital pseudonyms."[43]

---

[41] Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 Ga. L. Rev. 1, 8-10 (2006).

[42] Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex. L. Rev. 553 (1998).

[43] Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, in *Technology and Privacy: The New Landscape* 123, 125, 128 (Philip E. Agre & Marc Rotenberg, eds., 1997).

4. GOVERNANCE BY PROPERTY

A number of commentators propose that privacy can be protected by restructuring the property rights that people have in personal information. For example, according to Richard Murphy, personal information "like all information, is property." He goes on to conclude:

> . . . [I]n many instances, privacy rules are in fact implied contractual terms. To the extent that information is generated through a voluntary transaction, imposing nondisclosure obligations on the recipient of the information may be the best approach for certain categories of information. The value that information has ex post is of secondary importance; the primary question is what is the efficient contractual rule. Common-law courts are increasingly willing to impose an implied contractual rule of nondisclosure for many categories of transactions, including those with attorneys, medical providers, bankers, and accountants. Many statutes can also be seen in this light — that is, as default rules of privacy. And an argument can be made for the efficiency of a privacy default rule in the generic transaction between a merchant and a consumer.[44]

Lawrence Lessig also contends that privacy should be protected with property rights. He notes that "[p]rivacy now is protected through liability rules — if you invade someone's privacy, they can sue you and you must then pay." A "liability regime allows a taking, and payment later." In contrast, a property regime gives "control, and power, to the person holding the property right." Lessig argues: "When you have a property right, before someone takes your property they must negotiate with you about how much it is worth."[45]

Other commentators critique the translation of privacy into a form of property right that can be bartered and sold. For example, Katrin Schatz Byford argues that viewing "privacy as an item of trade . . . values privacy only to the extent it is considered to be of personal worth by the individual who claims it." She further contends: "Such a perspective plainly conflicts with the notion that privacy is a collective value and that privacy intrusions at the individual level necessarily have broader social implications because they affect access to social power and stifle public participation."[46]

Consider Pamela Samuelson's argument as to why property rights are inadequate to protect privacy:

> . . . Achieving information privacy goals through a property rights system may be difficult for reasons other than market complexities. Chief among them is the difficulty with alienability of personal information. It is a common, if not ubiquitous, characteristic of property rights systems that when the owner of a property right sells her interest to another person, that buyer can freely transfer to third parties whatever interest the buyer acquired from her initial seller. Free alienability works very well in the market for automobiles and land, but it is far

---

[44] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381, 2416-17 (1996).

[45] Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999).

[46] Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 Rutgers Computer & Tech. L.J. 1 (1998). For an argument about the problems of commodifying certain goods and of viewing all human conduct in light of the market metaphor, see Margaret Jane Radin, *Contested Commodities* (1996).

> from clear that it will work well for information privacy. . . . Collectors of data may prefer a default rule allowing them to freely transfer personal data to whomever they wish on whatever terms they can negotiate with their future buyers. However, individuals concerned with information privacy will generally want a default rule prohibiting retransfer of the data unless separate permission is negotiated. They will also want any future recipient to bind itself to the same constraints that the initial purchaser of the data may have agreed to as a condition of sale. Information privacy goals may not be achievable unless the default rule of the new property rights regime limits transferability. . . .
>
> . . . From a civil liberties perspective, propertizing personal information as a way of achieving information privacy goals may seem an anathema. Not only might it be viewed as an unnecessary and possibly dangerous way to achieve information privacy goals, it might be considered morally obnoxious. If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights. . . .[47]

Daniel Solove also counsels against protecting privacy as a form of property right because the "market approach has difficulty assigning the proper value to personal information":

> . . . [T]he aggregation problem severely complicates the valuation process. An individual may give out bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information. It is the totality of information about a person and how it is used that poses the greatest threat to privacy. As Julie Cohen notes, "[a] comprehensive collection of data about an individual is vastly more than the sum of its parts." From the standpoint of each particular information transaction, individuals will not have enough facts to make a truly informed decision. The potential future uses of that information are too vast and unknown to enable individuals to make the appropriate valuation. . . .
>
> [Property rights] cannot work effectively in a situation where the power relationship and information distribution between individuals and public and private bureaucracies is so greatly unbalanced. In other words, the problem with market solutions is not merely that it is difficult to commodify information (which it is), but also that a regime of default rules alone (consisting of property rights in information and contractual defaults) will not enable fair and equitable market transactions in personal information. . . .[48]

In contrast to these skeptics, Paul Schwartz develops a model of propertized personal data that would help fashion a market for data trade that would respect individual privacy and help maintain a democratic order. Schwartz calls for "limitations on an individual's right to alienate personal information; default rules that force disclosure of the terms of trade; a right of exit for participants in the market; the establishment of damages to deter market abuses; and institutions to police the personal information market and punish privacy violations." In his judgment, a key element of this model is its approach of "hybrid inalienability"

---

[47] Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan. L. Rev. 1125, 1137-47 (2000).

[48] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393 (2001).

in which a law allows individuals to share their personal information, but also places limitations on future use of the information. Schwartz explains:

> This hybrid consists of a use-transferability restriction plus an opt-in default. In practice, it would permit the transfer for an initial category of use of personal data, but only if the customer is granted an opportunity to block further transfer or use by unaffiliated entities. Any further use or transfer would require the customer to opt in — that is, it would be prohibited unless the customer affirmatively agrees to it.
>
> As an initial example concerning compensated telemarketing, a successful pitch for Star Trek memorabilia would justify the use of personal data by the telemarketing company and the transfer of it both to process the order and for other related purposes. Any outside use or unrelated transfers of this information would, however, require obtaining further permission from the individual. Note that this restriction limits the alienability of individuals' personal information by preventing them from granting one-stop permission for all use or transfer of their information. A data processor's desire to carry out further transfers thus obligates the processor to supply additional information and provides another chance for the individual to bargain with the data collector. . . .
>
> To ensure that the opt-in default leads to meaningful disclosure of additional information, however, two additional elements are needed. First, the government must have a significant role in regulating the way that notice of privacy practices is provided. As noted above, a critical issue will be the "frame" in which information about data processing is presented. . . .
>
> Second, meaningful disclosure requires addressing what Henry Hansmann and Reinier Kraakman term "verification problems." Their scholarship points to the critical condition that third parties must be able to verify that a given piece of personal information has in fact been propertized and then identify the specific rules that apply to it. As they explain, "[a] verification rule sets out the conditions under which a given right in a given asset will run with the asset." In the context of propertized personal information, the requirement for verification creates a role for nonpersonal metadata, a tag or kind of barcode, to provide necessary background information and notice.[49]

Finally, consider what Warren and Brandeis said about privacy as a property claim:

> The aim of [copyright] statutes is to secure to the author, composer, or artist the entire profits arising from publication. . . .
>
> But where the value of the production is found not in the right to take the profits arising from publication, but in the peace of mind or the relief afforded by the ability to prevent any publication at all, it is difficult to regard the right as one of property, in the common acceptation of that term.[50]

---

[49] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056, 2098-99 (2004). *See also* Vera Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. Davis L. Rev. 379 (2003) (although a collector may have rights in individuals' personal information, a property approach would correctly subordinate these rights to the rights of the individuals).

[50] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

5. GOVERNANCE BY STATUTORY REGULATION

Numerous statutes are directly and potentially applicable to the collection, use, and transfer of personal information by commercial entities. Congress's approach is best described as "sectoral," as each statute is narrowly tailored to particular types of businesses and services. The opposite of sectoral in this context is omnibus, and the United States lacks such a comprehensive statute regulating the private sector's collection and use of personal information. Such omnibus statutes are standard in much of the rest of the world. All member nations of the European Union have enacted omnibus information privacy laws.

In the United States, sectoral laws also do not regulate all commercial entities in their collection and use of personal information. Thus far, federal statutes regulate three basic areas: (a) entertainment records (video and cable television); (b) Internet use and electronic communications; and (c) marketing (telemarketing and spam). As you examine the existing statutes, think about the kinds of commercial entities that the law does not currently regulate. Consider whether these entities should be regulated. Also consider whether one omnibus privacy law can adequately apply to all commercial entities. Would the differences between types of commercial entities make a one-size-fits-all privacy law impractical?

The sectoral statutes embody the Fair Information Practices originally developed by HEW and incorporated into the Privacy Act. However, not all statutes embody all of the Fair Information Practices. As you study each statute, examine which of the Fair Information Practices are required by each statute and which are not.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

In several cases, plaintiffs have attempted to use the Electronic Communications Privacy Act (ECPA) to prevent certain kinds of information collection, use, and disclosure by commercial entities. Recall from Chapter 3 that EPCA consists of three acts: (1) the Wiretap Act, 18 U.S.C. §§ 2510–2522, which regulates the interception of communications; (2) the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2711, which regulates communications in storage and ISP subscriber records; and (3) the Pen Register Act, 18 U.S.C. §§ 3121–3127, which regulates the use of pen register and trap and trace devices. The attempts to use ECPA to regulate commercial entities using personal information primarily seek to use the Wiretap Act or the SCA.

IN RE PHARMATRAK, INC. PRIVACY LITIGATION

220 F. Supp. 2d 4 (D. Mass. 2002)

TAURO, J. Plaintiffs . . . bring this consolidated action against Pharmatrak, Inc. and several pharmaceutical companies. . . .

Plaintiffs allege that Defendants "secretly intercepted and accessed Internet users' electronic communications with various health-related and medical-related Internet Web sites and secretly accessed their computer hard drives in order to collect private information about their Web browsing habits [and] confidential health information without their knowledge, authorization, or consent." Plaintiffs contend that the Pharmaceutical Defendants conspired with Plaintiff Pharmatrak to "collect and share this wrongfully obtained personal and sensitive information." This activity was allegedly accomplished through the use of "web bugs," "persistent cookies," and other devices.

The Pharmaceutical Defendants hired Defendant Pharmatrak to monitor their corporate web sites and provide monthly analysis of web site traffic. . . . Pharmatrak specifically represented to the Pharmaceutical Defendants that these products did not collect "personally identifiable information." Even though the Pharmaceutical Defendants may not have known precisely how Pharmatrak's software worked, Plaintiffs readily admit that "the Pharmaceutical Defendants did authorize Pharmatrak's presence upon their Web sites."

---

[54] Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 Houston L. Rev. 751, 752-53, 768-69, 775-76 (2001).

Pharmatrak's system operated through the use of HTML programming, JavaScript programming, cookies, and "web bugs." Each of the Pharmaceutical Defendants' web pages were programmed with Pharmatrak code, which allowed Pharmatrak to monitor web site activity. When a computer browser requested information from a Pharmaceutical Defendant's web page, the web page would send the requested information to the user, and the site's programming code would instruct the user's browser to contact Pharmatrak's web server and retrieve a "clear GIF" from it. A clear GIF is a one pixel-by-one pixel or two pixels-by-two pixels graphic image, and is sometimes called a web bug or a "pixel tag." The purpose of a clear GIF was to cause the user's computer browser to communicate directly with Pharmatrak's web server. . . .

Having caused the user's Internet browser to contact Pharmatrak, Pharmatrak then sent a cookie back to the browser. A cookie is an electronic file "attached" to a user's computer by a computer server. Plaintiffs concede that "[c]ookies generally perform many convenient and innocuous functions." Commonly, cookies are used to store users' preferences and other information, which allows users to easily access and utilize personalized services on the web or to maintain an online "shopping cart." Cookies also allow web sites to differentiate between users as they visit by assigning each individual browser a unique, randomly generated numeric or alphanumeric identifier. If an individual browser had already visited the "Pharmatrak-enabled" website, Pharmatrak would recognize the previously placed cookie and could therefore differentiate between a repeat visit and an initial visit. . . .

Plaintiffs allege that the JavaApplet used by Pharmatrak allowed Pharmatrak to monitor the length of time that a particular user viewed one of the Pharmaceutical Defendants' web pages. Plaintiffs also allege that the JavaScript programming allowed Pharmatrak to "intercept the full URL of the tracked Web page visited by the user," as well as "the full URL of the Web page visited by the Internet user *immediately prior* to the user's visit to the Pharmatrak-coded Web page. This prior Web page address is known as a 'referrer URL.'" According to Plaintiffs, Pharmatrak used JavaScript "to extract referring URLs from the client's history, thereby bypassing any security or privacy mechanisms put in place to control the flow of potentially sensitive data." The JavaScript and JavaApplet, therefore, also caused users' computer browsers to communicate with Pharmatrak's server while they intentionally communicated with the Pharmaceutical Defendants' servers.

The examination of Pharmatrak's logs "identified hundreds of people by name." . . . Plaintiffs claim that Pharmatrak collected information which included: names, addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, and occupations. Pharmatrak also collected data about email communications, including user names, email addresses, and subject lines from emails. . . .

In sum, Plaintiffs argue that "Pharmatrak's technology permits defendants to collect extensive, detailed information about plaintiffs and Class members." In addition to the personal information discussed above, the information collected allegedly included "Web sites the Internet users were at prior to the time they went to the Pharmaceutical Defendants' Web sites, questions they asked and

typed in at those prior sites, information they entered while at the Pharmaceutical Defendants' web sites, and the types of computers they were using."

Title I of the Electronic Communication Privacy Act of 1986 ("ECPA"), Interception of Electronic Communications ("The Wiretap Act"), provides that:

> Except as otherwise specifically provided in this chapter[,] any person who — (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept, any wire, oral, or electronic communication . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5). 18 U.S.C. § 2511(1)(a).

This criminal statute provides for a private right of action, and is subject the following statutory exception:

> (d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act. 18 U.S.C. § 2511(2)(d).

Plaintiffs argue that Defendants intentionally "intercepted plaintiffs' or Class members' electronic communications with the Web sites they visited without plaintiffs' or the Class' [sic] knowledge, authorization, or consent. . . ."

Plaintiffs claim that "Pharmatrak intercepted plaintiffs' transmission of their personal information to the Pharmaceutical Defendants' Web sites without the express or implied consent of either plaintiffs or the Pharmaceutical Defendants." Despite the fact that the Pharmaceutical Defendants may have consented to Pharmatrak's assembly of anonymous, aggregate information, Plaintiffs insist that the web sites never consented to Pharmatrak's collection of personally identifiable information. Absent this specific consent, Plaintiffs argue, the Wiretap Act's statutory exception simply does not apply. . . .

In the present case, Plaintiffs concede that the Pharmaceutical Defendants consented to the placement of code for Pharmatrak's . . . service on their web sites. . . . [C]onsent precludes a claim under the Wiretap Act. The Pharmaceutical companies contracted with Pharmatrak, and authorized Pharmatrak to communicate with any users who contacted the Pharmaceutical Web sites. . . . It is sufficient that the Pharmaceutical Defendants were parties to communications with Plaintiffs and consented to the monitoring service provided by Defendant Pharmatrak.

Plaintiffs are also unable to demonstrate that Defendants acted with a tortious purpose. Plaintiffs have produced no evidence "either (1) that the primary motivation, or (2) that a determinative factor in the actor [Pharmatrak's] motivation for intercepting the conversation was to commit a criminal [or] tortious . . . act." Without a showing of the requisite *mens rea,* Plaintiffs cannot succeed on their claim under the Wiretap Act. . . .

Title II of the ECPA, also known as the "Stored Wire and Electronic Communications and Transactional Records Act," "aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications." The statute provides:

> [W]hoever — (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided by subsection (b) of this section. 18 U.S.C. § 2701(a).

Plaintiffs acknowledge that § 2701 was primarily designed to provide a cause of action against computer hackers, and argue that "Defendants' conduct of accessing data in plaintiffs' computers, including the content of plaintiffs' e-mails, constitutes electronic trespassing and falls squarely within the ambit of Section 2701."

Defendants disagree, and claim that they are entitled to summary judgment on at least two separate grounds: (1) Plaintiffs' computers are not facilities which provide electronic communications services, an essential element of § 2701; and (2) any alleged access to "communications" was authorized.

Defendants are correct that an individual Plaintiff's personal computer is not a "facility through which an electronic communication service is provided" for the purposes of § 2701. Plaintiffs find it noteworthy that "[p]ersonal computers provide consumers with the opportunity to access the Internet and send or receive electronic communications," and that "[w]ithout personal computers, most consumers would not be able to access the Internet or electronic communications." Fair enough, but without a telephone, most consumers would not be able to access telephone lines, and without televisions, most consumers would not be able to access cable television. Just as telephones and televisions are necessary devices by which consumers access particular services, personal computers are necessary devices by which consumers connect to the Internet. While it is possible for modern computers to perform server-like functions, there is no evidence that any of the Plaintiffs used their computers in this way. While computers and telephones certainly provide services in the general sense of the word, that is not enough for the purposes of the ECPA. The relevant *service* is Internet access, and the service is provided through ISPs or other servers, not though Plaintiffs' PCs.

Even if the court were to assume that Plaintiffs' computers are "facilities" under § 2701, any access to stored communications was authorized and, thus, Defendants' conduct falls under the exception from liability created by § 2701(c)(2). . . . [T]he Pharmaceutical Defendants are "users" under the ECPA. . . . As users, the Pharmaceutical Defendants could consent to Pharmatrak's interception of Plaintiffs' communications. . . .

In addition, the ECPA does not prohibit Pharmatrak's actions with regard to the placing of cookies on Plaintiffs' computers. Section § 2701 seeks to target communications which are in "electronic storage" incident to their transmission. . . . "Title II only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to store it." Even if such cookies were covered by the ECPA, Pharmatrak created and sent the cookies, and thus any accessing of the cookies by Pharmatrak at a later date would certainly be "authorized." Because Pharmatrak's cookies fall outside the scope of § 2701, Plaintiffs' claim under that section must fail. . . .

NOTES & QUESTIONS

1. ***Postscript.*** On appeal, the First Circuit let stand the district court's holding dismissing the plaintiff's Stored Communications Act claim. *In re Pharmatrak, Inc. Privacy Litigation,* 392 F.3d 9 (1st Cir. 2003). As for the Wiretap Act claim, the court reversed. To prove a violation of the Wiretap Act, the court stated, the plaintiff must prove that "a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." The court concluded that the "district court made an error of law . . . as to what constitutes consent." The court reasoned that the "client pharmaceutical companies did not give the requisite consent. The pharmaceutical clients sought and received assurances from Pharmatrak that its . . . service did not and could not collect personally identifiable information. . . . Nor did the users consent." The court remanded as to whether the interception had been intentional.

   Note that there was no consent here because Pharmatrak didn't adequately inform its pharmaceutical clients. Suppose that Pharmatrak told its pharmaceutical clients that it was gathering personal information, but that Pharmatrak did not inform the individual users of the pharmaceutical websites. Would the consent exception apply under these circumstances?

   On remand, the district court concluded that the interception was not intentional, and that at most, Pharmatrak had negligently gathered the personal data. Accordingly, the Wiretap Act claim was again dismissed. *In re Pharmatrak, Inc. Privacy Litigation,* 292 F. Supp. 2d 263 (D. Mass. 2003).