May 24, 1999

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, N. W.
Washington, D.C. 20580

RE: Children's Online Privacy Protection Rule – Comment, P994504

Dear Secretary:

I submit the following comments in response to the Commission's Notice of Proposed Rulemaking to Implement the Children's Online Privacy Protection Act of 1998. These remarks respond to the first General Question posed by the Commission, soliciting comments on provisions in the proposed Children's Online Privacy Protection Rule (the "Rule").

Notice Provisions

The proposed Rule requires operators who wish to collect and use information about children to convey some information that the operators may want consumers to receive and other information that they may not wish consumers to act on. In researching informational privacy for a forthcoming article in the Washington Law Review, I found that firms that wish to communicate information to consumers behave differently from firms obliged to convey messages that they do not in fact wish consumers to act on.[1] That has implications for the design of rules governing notice.

The article argues that because some businesses can use information about consumers in various ways, including increasing their own sales and selling the information to others, they have incentives to make it difficult for consumers to protect their privacy. I also assert that businesses have the ability to increase consumers' transaction costs in protecting their privacy in a number of ways. The article further suggests that some marketers do in fact inflate the transaction costs incurred by consumers, and that many consumers, faced with significant transaction costs and certain constraints common to consumers, decide not to protect their privacy, even though they would choose differently if it were easier to do so.

---

[1] The article, scheduled for publication in the Washington Law Review in the fall of 1999, is titled *Opting In, Opting Out, Or No Options at All: The Fight for Control of Personal Information* (the "article"). The article is copyrighted by the Washington Law Review. The Law Review has given me permission to submit a copy of the enclosed article as part of my comments on the Rule. The article has not yet been edited by the Washington Law Review and does not necessarily reflect the views of the Washington Law Review or St. John's University School of Law.

For example, certain businesses are required by law to notify consumers of their information practices so consumers have the opportunity to prevent the sale or use of their personal information.[2] Some of these businesses increase consumer transaction costs in protecting privacy by, among other things, obscuring information about privacy by providing it along with other information which consumers will find of greater interest; providing the privacy information in lengthy documents; using language consumers find difficult to understand; and requiring consumers to communicate their privacy preferences by creating an original writing (as opposed to using company-supplied forms or telephone communications, which the companies permit the consumer to use when providing information the companies wish to receive).[3]

On the other hand, in at least one instance described in the article, when a business was prohibited from using consumer information without obtaining consumer consent, the business aggressively sought consumer consent by calling and sending attractive mailings to customers, establishing a toll-free number for consumers with questions, sending customers a printed form with a postage paid envelope, and offering incentives to consumers who signed up.[4]

Section 312.5(a) of the Proposed Rule requires operators using information about children to obtain permission from parents in most instances before collecting or using the information. Because operators will wish to receive such permission, they will have no incentive to make it difficult for consumers to provide it. However, the Rule also requires operators using information about children to provide parents with statements the operators may not wish parents to act on, such as the parental right to review personal information provided by the child, §§ 312.4(b)(2)(vi), 312.6, that information may be furnished to third parties, § 312.4(b)(2)(iv), and that the parent may agree to the collection and use of the child's information without consenting to disclosure to third parties, § 312.5(a)(2). If online companies behave as other businesses have, they may attempt to obscure the disclosures required by §§ 312.4(b)(2)(iv), 312.4(b)(2)(vi), 312.5(a)(2), and 312.6.

Section 312.4(a) requires that notices required under the Rule "must be clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory materials." That standard might be inadequate. The similar "clear and conspicuous" standard for disclosures under the FCRA that information may be shared among affiliates[5] appears not to have done the trick. As stated in the article at p. 66:

[t]he Office of the Comptroller of the Currency is reported to have found that "few banks

---

[2] *See, e.g.* Cable Communications Policy Act of 1984, as amended by the Cable Television Consumer Protection and Competition Act of 1992, 47 U.S.C. §§521 (cable television companies may not sell their subscriber lists unless they give subscribers the opportunity to opt-out); Fair Credit Reporting Act, 15 U.S.C. § 1681a(d)(2)(A)(iii) (defining "consumer report" as excluding "any communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons" which has the effect of excepting such communications from regulation by the FCRA).

[3] *See* article at pp. 62-68.

[4] The prohibition on use of customer information without permission is contained in interpretations by the Federal Communications Commission of the Telecommunications Act of 1996, and appears at 63 Fed. Reg. 20,326. It is discussed in the article at page 82.

[5] *See supra* note 2.

highlight this option."[6] Then-Acting Comptroller of the Currency Julie Williams has commented that "Most bank customers can't ever recall seeing something like this."[7] And, she has observed:

> it has been known to happen that the affiliate-sharing "opt-out" disclosure is buried in the middle or near the end of a multi-page account agreement. For existing accounts, some institutions have gotten into the habit of reducing the required "opt out" disclosures to the fine print along with a long list of other required disclosures. Few consumers are likely to have the fortitude to wade through this mass of legal verbiage, and fewer still will take the time to write the required "opt out" letter. I have even heard of people getting two separate notifications covering different types of information, requiring two separate letters to opt out.[8]

A better approach might be to harness the disclosures firms will not want to make to the disclosures they do want to make, by specifying in the Rule that disclosures provided under §§ 312.4(b)(2)(iv), 312.4(b)(2)(vi), 312.5(a)(2), and 312.6 must be at least as conspicuous and easy to understand as attempts to secure parental consent under § 312.5(a)(1). In addition, to prevent companies from overloading consumers with information, § 312.4(a) should be amended to provide that notices should be no longer than reasonably necessary.

An additional issue raised by § 312.4(a) is the question of to whom the notices are understandable or confusing. In deception matters, the Commission, of course, currently uses the standard articulated in the 1983 Policy Statement and implemented in *In re* Cliffdale Associates, 103 F.T.C. 110 (1984) of "likely to mislead consumers acting reasonably under the circumstances." On the other hand, some courts implementing the Fair Debt Collection Practices Act have used the "least sophisticated consumer" test, *see* Clomon v. Jackson, 988 F.2d 1314, 1318-20 (2d Cir. 1993), or the similar "unsophisticated consumer" test, *see* Gammon v. GC Servs. Ltd. Partnership, 27 F.3d 1254, 1257 (7th Cir. 1994). It would be helpful if the Commission would clarify this issue with respect to § 312.4(a). My own preference is for the least sophisticated consumer test, given the liberties firms have already taken in this area, and the difficulties some consumers have in addressing privacy issues, as discussed in the article.

Section 312.5(a)(2)

---

[6] Leslie Wayne, P*rivacy Matters: When Bigger Banks Aren't Bettter,* NY Times, Oct. 11, 1998, § 4, at 4.

[7] Leslie Wayne, P*rivacy Matters: When Bigger Banks Aren't Bettter,* NY Times, Oct. 11, 1998, § 4, at 4.

[8] Remarks by Julie L. Williams, Acting Comptroller of the Currency before the Banking Roundtable Lawyers Council (May 8, 1998), available at <http://www.occ.treas.gov/ftp/release/98%2D50a.txt> (last checked Oct. 13, 1998). *See also* Remarks by Julie L. Williams Before the Consumer Bankers Association (Oct. 26, 1998) available at <http://www.occ.treas.gov/ftp/release/98-109a.txt> (last checked Nov. 11, 1998):

> We can find too many disclosure statements that lack specificity, clarity, and simplicity. They are too often opaque and obscure, rather than 'clear and conspicuous.' They place the burden on customers to provide a long list of information, including, in at least one case, account numbers for each account for which information is not to be shared. Too often we found disclosure information in fine print, buried in a mass of equally tiny type, along with other required terms and disclosures. In short, we continue to find that consumer anxieties--based on the lack of clarity and consistency in banks' disclosure policies and practices--are not entirely unfounded.

Because some operators may wish to make it as easy as possible for parents to consent to the use of their children's information, it is likely that some operators wishing to use children's information will send parents forms to complete and return. Operators that wish to sell information about children will sometimes have no incentive to simplify the task of parents who wish to consent to use of their children's information, but not allow disclosure to third parties. Indeed, such operators may have an incentive to do as little as possible to comply with § 312.5(a)(2)'s requirement that the operator give the parent the option to consent to collection and use of the child's personal information but not disclosure to third parties. Thus, an operator could conceivably create a form for parents to use to consent to the sale of information, but comply with § 312.5(a)(2) by telling parents they may communicate their objections to sale in a separate letter, in the hope that some parents will not make the effort to send the letter. Consequently, the Rule should also provide that operators who wish to disclose children's information to others, and use forms, have a place for parents to check to indicate that they do not consent to disclosure of information to third parties, even though they may agree to collection and use of the child's information for internal purposes.

Similarly, some operators may allow consumers to express their wishes through telephone calls. To avoid the same problem, the Rule should provide that when parents consent to the collection and use of their child's information in telephone calls, operators should explain at that time that the parent may refuse to allow the disclosure of the information to third parties, and ask whether the parent wishes to do so.

Section 312.5(c)(3)

Section 312.5(c)(3) provides that in some circumstances operators can dispense with verifiable personal consent from the parent if the operator makes reasonable efforts to ensure that the parent receives notice. Mechanisms to provide such notice are defined as included sending the notice to the parent's e-mail address. Operators in such circumstances may not want the parent to refuse, and so may attempt to comply with the Rule in such a way as to increase the likelihood that the parent would not read the e-mail, as for example, by making the e-mail message look like spam. Certainly many people delete messages that appear to be spam without reading them. To frustrate such attempts, the Rule could require the message line to contain information that would make it more likely that the parent would read the message. For example, the Rule could require the message header to contain the child's name.

Section 312.6

I have two suggestions relating to § 312.6. First, § 312.6 does not currently provide for a time limit for operators to comply with parental requests. It might be helpful to add that the operators must provide the information within a reasonable time, or within a specified number of days.

Second, § 312.6 does not currently require operators to give parents the option to receive statements about information collected concerning their child on an on-going basis. Many parents who consent to the collection of the information will probably forget about doing so, and will not remember to check back to see what information about their child has been collected and used. The Rule does not require operators to remind parents that the information-collection process is occurring. It probably would not be expensive for operators to provide parents (at least through e-mail for parents who have it) with regular statements containing the information

they collect about the child. The Rule should provide that operators collecting and using information about a child should, at the time the parents consent to the collection and use of the information, provide parents with the opportunity to request such periodic updates.

* * *

Thank you for this opportunity to comment on the Rule. I include a paper copy of the article, as well as a computer disk containing an electronic copy of this letter and the article. If you have any questions, my direct dial number is 718-990-6429, and my e-mail address is **Error! Reference source not found.**.

Respectfully submitted,

Jeff Sovern
Professor of Law

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

by Jeff Sovern[1]

I. Introduction

A few years ago one of my students told me that he had a copy of my driving record.[2] During a later class he asked if I wanted a list of my neighbors.[3] On other occasions he correctly

---

[1] Professor of Law, St. John's University School of Law. A.B., J.D., Columbia University. The author thanks John Q. Barrett, Philip D'Ancona, and Victor M. Serby. The author is also grateful to St. John's University School of Law for its research support.

[2] Driving records in New York are available to the public. *See* NY VTL § 508.3 ("The commissioner shall keep a record of every license issued which record shall be open to public inspection . . . ."). Businesses use driving records for a number of commercial purposes. For example, eyeglass sellers use them to identify for solicitation consumers who require corrective lenses. The information about height and weight in driving records is useful to clothing retailers, especially those that sell to the "big and tall" market. *See* Michael W. Miller, *Firms Peddle Information From Driver's Licenses*, Wall St. J., Nov. 25, 1991 at B1. Some states make a significant amount of money from selling drivers' information. *See What's in a Name? Big Bucks*, Albany Times Union, May 8, 1996 at A14 (state sold list of drivers for $1.4 million); Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 150 (1996). Nevertheless, some states do not release the data while others use an opt-out procedure under which drivers have the opportunity to prevent disclosure of their information. *Id*. In 1994 Congress enacted the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-25, to restrict access to information in state motor vehicle records. In twelve subsections, it lists permissible purposes for use of a driver's personal information. 18 U.S.C. § 2721(b)(1)-(10), (13), (14). It also provides in two additional subsections that a consumer's information may be used for "bulk distribution for surveys, marketing or solicitations" or for "any other use" if the motor vehicle department has notified consumers "in a clear and conspicuous manner" that the information may be used for such purposes and given consumers the opportunity to prohibit disclosures for such purposes. 18 U.S.C. § 2721(b)(11), (12). This statute has not prevented the existence of an internet site that lists driver's license information, as discussed *infra* in note ___. The federal statute was ruled an unconstitutional infringement on the powers of the states under the Tenth Amendment in Condon v. Reno, 155 F.3d 453 (4th Cir. 1998). *But see* Oklahoma v. United States, 161 F.3d 1266 (10th Cir. 1998) (upholding statute); Travis v. Reno, 163 F.3d 1000 (7th Cir. 1998) Pryor v. Reno, 998 F. Supp. 1317 (M. D. Ala. 1998) (same). For an argument that government may not constitutionally restrict the reporting of or access to information contained in public records, see Cheryl M. Sheinkopf, *Balancing Free Speech, Privacy and Open Government: Why Government Should Not Restrict the Truthful Reporting of Public Record Information*, 44 UCLA L.Rev. 1567 (1997).

[3] This information is available in a computer database. The information is useful to creditors searching for a debtor who has moved. The database allows the creditor to identify the debtor's former neighbors, so that the creditor can ask them the debtor's new whereabouts. William M. Bulkeley, *Technology*, Wall St. J., Sept. 10, 1991, at B1.

told me the name of one of my brothers and who the lienholder is on my co-op apartment. Once he gave me a bullet.[4] Though the story is a little frightening, this was hardly an obsession for him; rather, he was just having some fun, sandwiched between the demands of class and work.[5] Someone for whom it was an obsession--or for whom the information was valuable enough to make it worth serious exploration-- undoubtedly could have learned much more.[6]

The information available about consumers is striking. For example, you can buy lists of people who have bought skimpy swimwear and related items such as clingy short dresses and skirts, gambling Arabs, college students sorted by major, class year and tuition payments, millionaires and the people who live near them, people who just lost a loved one, male buyers of fashion underwear, women who buy wigs, callers to a 900-number national dating service, rocket scientists, children who subscribe to magazines or sent in rebate forms included with toys, people who have their urine tested, medical malpractice plaintiffs, workers' compensation claimants, people who have been arrested for--but not convicted of--crimes, impotent middle-aged men, epileptics, people with bladder-control problems, buyers of hair removal products or tooth whiteners, people with bleeding gums, high-risk gamblers, people who have been rejected for bank cards, and tenants who have sued landlords.[7] There are lists based on ethnicity, political

---

[4] He had cut the bullet open, removed the gunpowder, and taped it together again, thus rendering it an inert piece of metal, but it does kind of make you wonder. The student in question graduated, passed the bar, made it through the Character Committee, and is now practicing law. That makes you wonder too.

[5] The zeal of some law students to learn more about their professors is not new; in the fictional movie "The Paper Chase," one law student went to far as to read notes his professor had made as a law student. On the other hand, many if not most, law students are not particularly interested in information about their professors (fortunately). One student, speaking for a number of her peers, suggested that the student who had probed the computer about me "get a life."

[6] Though this student was not stalking me, stalking, including cyberstalking, is a more prevalent problem than is widely understood. A recent study concluded that each year one million women and 400,000 men are victims of stalkers. *See* Jane E. Brody, *Researchers Unravel the Motives of Stalkers,* N. Y. Times, Aug. 25, 1998, at F1.

[7] *See Merchants of Data--Are They Telling on You?* Consumer Reports 356 (May 1991); *Your Health Files--How Insurers Check*, Consumer Reports 357 (May 1991); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497, 519-20, 523 (1995) (hereinafter, Reidenberg, *Setting Standards*; H. Jeff Smith, *Managing Privacy* 100 (1994); Larry Tye, *List-makers Draw a Bead on Many*,

opinions, and sexual orientation.[8]

The media are filled with horror stories about the use of personal information. Stories routinely appear on the availability of information most people consider confidential.[9] A television reporter--without any proof of identification--obtained overnight a list of 5,000 families, including addresses and the names of children, for a $277 money order. The reporter used the name of Richard Allen Davis, then on trial for kidnapping and killing a twelve-year old.[10]

Some reports are so overwhelming as to be mind-numbing. One company supposedly

---

Boston Globe, Sept. 6. 1993 at 1; Oscar H. Gandy, Jr., *The Panoptic Sort* 91 (1993); Robert O'Harrow Jr., *For Sale on the Web: Your Financial Secrets Bank Accounts Vulnerable to Data Brokers*, Wash. Post, June 11, 1998, at A01; Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 322 (1996); Erik Larson, *The Naked Consumer* 63-64, 93 (1992); U.S. Dept. of Commerce, National Telecommunications & Information Administration, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* A-3 (1995 App.).

[8] U.S. Dept. of Commerce, NTIA, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* A-3 (1995 App.) ("list brokers have created catalogs of 'Arabs, in Their Native Lands, Who Gamble and Invest;' 'Doctors Who Are Known to Have Gambled;' and 'Jewish Philanthropists and Investors.'"); Martin J. Smith, *Ever Wonder Why You Get All That Unsolicited Junk Mail?* Arizona Republic, Dec. 5, 1993, at A1 (noting that 1.85 million name Hispanic New Movers File is available at a rate of $70 per thousand names); Larry Tye, *List-makers Draw a Bead on Many*, Boston Globe, Sept. 6. 1993 at 1 (lists of those with Italian lineage, Japanese lineage, Jewish lineage); Mary Zahn & Eldon Knoche, *Electronic Footprints: Yours are a Lot Easier to Track Than You May Think*, Milwaukee Sentinel, Jan. 16, 1995, at 1A (list of subscribers to gay and lesbian magazines; company claims to be able to identify 85% of the 2.6 million Jewish households in the United States); Reidenberg, *Setting Standards supra*, note ___ at 519-20, 523; Susan Headden, *The Junk Mail Deluge*, U.S. News & World Rep., Dec. 8, 1997.

[9] *See, e.g.*, Margot Williams & Robert O'Harrow, Jr., *OnLine Searches Fill in Many Holes*, Wash. Post, March 8, 1998 at A19, available on web at <http://www.washingtonpost.com/wp-srv/frompost/march98/sidebars/kaplan8.htm> (last checked June 15, 1998) (free service on web found consumer's address, phone number, names and addresses of 20 neighbors, and provided map and directions to consumer's home; another service provided for $9.50 consumer's previous addresses and for $12 consumer's social security number and birthday; another service provided driving record for $15.50; Lexis-Nexis charged $41 for information about consumer's home, including current assessed value, date of original purchase and price, number of square feet and rooms; another service provided sales estimates for consumer's business for $5; other services gave names and ages of consumer's children, and length of residence); Erik Larson, *The Naked Consumer* 58 (1992) ("they can know, for example, what brand of condoms you charged at your local Rite-Aid or that you picked up a pregnancy test today. They can know too about your secret life, the flowers you buy that your wife never sees, your practice of staying in gay guest houses whenever you go away on business.").

[10] Evan Hendricks, *Metromail Stung Again*, Privacy Times, May 17, 1996, at 4. *See also* Ann Reilly Dowd, *Protect Your Privacy*, Money Mag., Aug. 1, 1997 ("Marketing information about kids is now a hot commodity and for good reason. . . . For 8.5 [cents] a name and a copy of the script you'll use to sell your product to kids, one Tucson company, for example, will give you as many as 8 million children under 17 sorted by name, sex, age and city.").

claims to have identified a market segment for every household in the United States,[11] while another advertises that its database lists every registered voter, as well as their telephone numbers, addresses, and ethnic surname identification.[12] A business executive estimates that on a normal day the average American's personal information moves from one computer to another five times.[13] The typical person is said to appear in anywhere from 25 to 100 databases.[14] A person sued a marketing company, only to discover that their dossier on her is 25 pages long.[15] The computer library of an information service few have even heard of, Acxiom Corp., is reported to have 350 trillion characters of consumer data on more than 195 million Americans.[16] Services peddle bank account balances,[17] unlisted telephone numbers, and salary figures.[18] In Joel Reidenberg's words, the "private sector has precisely the type of dossiers that the public has long feared government would abuse."[19]

---

[11] Gandy, supra note ___ at 92 (1993). The Department of Commerce has reported on a company that has a database with information on more than 150 million people and 90 million households and another company with a database on 133 million individuals. U.S. Dept. of Commerce, NTIA, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* A-2, n.10 (1995 App.).

[12] Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. Chi. Leg. F. 77, 96 *citing* advertisement by Aristotle Industries, Campaigns and Elections 83 (Feb. 1995).

[13] Robert Moskowitz, Protecting Your Privacy Requires Planning, Investor's Bus. Daily, Sept. 16, 1994, at 1. *See also* Jeffrey Rothfeder, *Privacy for Sale* 17 (1992).

[14] Andrew L. Shapiro, *Privacy for Sale: Peddling Data on the Internet*, The Nation, June 23, 1997 at 11, 12.

[15] Nina Bernstein, *Personal Files Via Computer Offer Money and Pose Threat,* N.Y. Times, June 12, 1997, at 1, B14 (company "retrieved more than 900 tidbits of Ms. Dennis's life going back to 1987. Laid out on 25 closely printed pages of spreadsheets were not only her income, marital status, hobbies and ailments, but whether she had dentures, the brands of antacid tablets she had taken, how often she had used room deoderizers, sleeping aids and hemorrhoid remedies.").

[16] Robert O'Harrow, Jr. *Are Data Firms Getting Too Personal?* Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy/8.htm> (last checked June 15, 1998); Michael Fraase, INFORMATION ECLIPSE: PRIVACY AND ACCESS IN AMERICA 155 (1999).

[17] Robert O'Harrow Jr., *For Sale on the Web: Your Financial Secrets Bank Accounts Vulnerable to Data Brokers*, Wash. Post, June 11, 1998, at A01; Robert Douglas, Al Schweizer & Boris Melnikoff, *How Your Financial Privacy is Threatened*, Consumers' Research Magazine, Dec. 1998 at 10.

[18] Nina Bernstein, *On Line, High-Tech Sleuths Find Private Facts*, N. Y. Times, Sept. 15, 1997, at A1, A20.

[19] Reidenberg, *Setting Standards supra* note ___ at 536.

Even the lists of lists are voluminous. A list directory describes more than 10,000 lists which can be purchased.[20] The Direct Marketing Association, a trade association, estimates that more than 15,000 consumer mailing lists exist, containing some two billion names, including, obviously, duplicates.[21] More than one thousand commercial services are said to broker lists.[22]

Not only is more personal information available than ever before, but it is becoming easier and less expensive to obtain access to it.[23] Internet sites and even Westlaw have databases designed to locate individuals and report on their transactions, including their bankruptcy records, lawsuits, liens, real property refinancings and transfers, and the location of their assets.[24]

---

[20] The *Standard Rate & Data Service, Direct Mail List Rates and Data* is referred to in Jill Smolowe, *Read This!!!!!!*, Time, Nov. 26, 1990, at 62, 66; and Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 Fed. Com. L. J. 195, 202 n.29 (1992). One company alone was recently reported to maintain 1,600 databases, containing more than 3.5 billion public records. Rajiv Chandrasekaran, *Doors Fling Open to Public Records,* Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy9.htm> (last checked June 15, 1998).

[21] Paula Crawford Squires, *Transactions Go Into a Database; Businesses Compile Dossiers on Customers*, Richmond Times Dispatch, July 28, 1996, at A-12.

[22] U.S. Dept. of Commerce, National Telecommunications and Information Administration, *Privacy and the NII: Safeguarding Telecommunications-Related Information* A-2 (1995 App.).

[23] *See, e.g.*, Evan Hendricks, *CDB's Cut-Rate Look-Up Service*, Privacy Times, Feb. 20, 1998, at 8 (cost of look-up service, which provides subject's names, alias names, current and prior addresses, telephone number, Social Security number, driver's license number, date of birth, links to possible relatives, real property ownership, bankruptcies, tax liens, judgments, corporations, UCC filings, and other information reduced to $7 per search); Nina Bernstein, *On Line, High-Tech Sleuths Find Private Facts*, N. Y. Times, Sept. 15, 1997, at A1, A20 (in less than three minutes and for about $1.50, service provides subscribers with Social Security number, date of birth, and telephone number for names typed in; "For a few minutes and a few dollars more, the computer screen fills with other personal details: past and current addresses, names and telephone numbers of neighbors, names and Social Security numbers of relatives, in-laws and business associates, civil judgments and property tax filings."); Kristin Davis, *Guarding Your Financial Privacy*, Kiplinger's Personal Finance Mag., Aug. 1995, at 38, 40 ("Among the . . . most voracious customers: employers, journalists and private detectives. 'I can do in one hour what ten years ago would have taken a week to do.'" said one private investigator); U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 4 (1995) ("because the costs associated with storing, processing, and distributing personal records are continuously decreasing, accumulating personal information from disparate sources will become a cost-effective enterprise for information users with interests ranging from law enforcement to direct marketing.").

[24] For information about Westlaw, *see* WESTLAW Database Directory 141-43 (1997). Among the Westlaw databases for locating individuals are eight bearing the prefix "People Finder". The suffixes read: "Address Alert," "Name Tracker," "Name-Tracker-Deceased," "Skip Tracer," "Social Security Number Tracker," "Social Security Number Tracker--Deceased," "Telephone Tracker," and "TRW/Trans Union Credit Bureau Headers Population Demographics." Among the internet sites which can be used to find people are Database America, which is at <http:/www.databaseamerica.com> (last checked Aug. 4, 1998). An internet site which provides information on assets, lawsuits, liens, bankruptcy records, refinancings, and other information is KnowX, located at <http://www.knowx.com> (last checked Aug. 4, 1998). Lexis/Nexis also has two services designed to locate people, P-Trak and P-Find. For discussion of what those services can do s*ee* FTC, Public Workshop on

Other internet sites list driver's license information and motor vehicle information, and verify social security numbers.[25] The number of websites selling personal information is estimated at several thousand.[26] Prices for many computer services are now at the point where information which formerly could be afforded only by businesses is now accessible to individuals.[27]

To be sure, access to some information--such as credit reports--is regulated, though that may be of small comfort to the various celebrities who have discovered their credit reports in the hands of writers.[28] Still other data, including much of that referred to in the preceding

---

Consumer Information Privacy, Session One: Database Study, at 18-29 (June 10, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Karen Welch, Strategic Account Consultant, Lexis-Nexis).

[25] *See* <http://www.ameri.com/dmv/dmv.htm> (driver's license information and motor vehicle information for every state; fee charged) (last checked May 8, 1998); <http://www.glr.com/stalk.html> (called "The Stalker's Home Page," this site contains links to sites verifying social security numbers and providing other information) (last checked May 8, 1998); <http://www.searchfirst.com> (last checked Nov. 3, 1998) (driver's license information, social security number verification, credit report, criminal records, available for various fees under $50); <http://www.informus.com> (last checked Nov. 3, 1998) (credit reports, social security number verification, credit reports, criminal records available for various fees under $25). *See also* Jerry Kleczka, *Protecting Your Social Security Number From Millions of Prying Eyes*, 19 At Home With Consumers, No. 1 at 2, 5 (May 1998) ("a significant number of World Wide Web sites sell Social Security numbers to anyone with a few dollars, a computer, and a telephone. . . . Most alarming is the Deep Data Web site, where anyone can purchase a 40-state search for an individual's Social Security number for as little as $20."); Andrew L. Shapiro, *Privacy for Sale: Peddling Data on the Internet*, The Nation, June 23, 1997 at 11 (writer obtained for free on the internet in about ten minutes Ted Turner's social security number, Rush Limbaugh's home address and phone numbers for Senator Robert Dole); Evan Hendricks, *Arizona Drivers' Credit Card Numbers Exposed on Internet*, Privacy Times, May 1, 1998, at 3 (credit card numbers of car owners mistakenly posted on web site for several months); Evan Hendricks, *Uproar Over DMV Net Posting Causes Oregonian to Duck*, Privacy Times, Aug. 21, 1996 at 1,2 (person purchased list of 3 million Oregon drivers' names and addresses for $222 and posted it on Website).

[26] Robert O'Harrow, Jr. *Are Data Firms Getting Too Personal?* Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy/8.htm> (last checked June 15, 1998) (estimate by Jack Reed, chair of Information Resource Service Co).

[27] *See* U.S. Dept. of Commerce, NTIA, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* A-7 & n.30 (1995 App.). Some information services provide the information to anyone who pays their fee. FTC, Public Workshop on Consumer Information Privacy, Session One: Database Study, at 45-46 (June 10, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Carol Lane) (information service available on internet without subscription).

[28] *See, e.g.*, Jeffrey Rothfeder, *Privacy for Sale* 17-21 (1992) (reporting on Vice President Quayle's accounts at Sears, Brooks Brothers, his social security number and Visa card number); Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues*, 12 J. Public Pol. & Marketing 106, 111 (1993) (writer obtained CBS News Anchorperson Dan Rather's credit report, charge card data, mortgage information, location of residence, shopping information, dining information, and how much he spends); *cf.* U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 4 (1995) (journalists discovered financial, legal, marital, and residential history of movie producer George Lucas and White House Chief of Staff Leon Panetta). *Cf.* Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection From Private and Commercial Intrusion*, 25 Fla. St. U. L. Rev. 25, 45 (1997)

paragraphs, are not subject to legal restraint. A service gave Erik Larson the home address of Baltimore's mayor, Kurt L. Schmoke, as well as the purchase price, mortgage amount, and taxes Mayor Schmoke paid on the property.[29] Jeffrey Rothfeder has described how after he obtained then-Vice President Dan Quayle's credit report, he was able, using techniques learned from a private investigator, to call a major retailer and persuade its credit department to tell him Quayle's home address and telephone number.[30] The Federal Reserve has noted that some internet information providers "place few, if any, restrictions on access or intended use of information, and may permit immediate access over the Internet."[31]

Businesses use the information available to them for a variety of purposes, the best known of which is to solicit sales. Thus, each year Americans are reported to receive sixty-three billion pieces of junk mail and billions of telemarketing calls.[32] But the information is also used for purposes which are less well known. For example, one company combined the data from a number of grocery stores to create a list of more than half a million supposedly weight-conscious consumers who had purchased yogurt, low-calorie breads, and similar products. The company marketed the list to sellers of fitness equipment, vitamins and clothing. It offered a list of "fancy food buyers"--consumers who bought refrigerated pastas or frozen yogurt--to travel magazines

---

("Credit bureau terminals are now in thousands of sites, including car dealerships, real estate offices and banks, providing easy access for information resellers. According to one source, no one has ever been prosecuted for illegally obtaining credit reports." "almost anything can be characterized as a legitimate business need" thus satisfying statutory standard for obtaining credit reports) (footnotes omitted). In 1997 new amendments to the Fair Credit Reporting Act went into effect, which may offer more protection for credit reports. *See* 15 U.S.C. § 1681 et seq.

[29] Erik Larson, *The Naked Consumer* 61 (1992).

[30] Jeffrey Rothfeder, *Privacy for Sale* 20-22 (1992). Rothfeder describes throughout his book the kind of information available about people, through lawful and unlawful means. Ultimately, the credit bureau which supplied Rothfeder with the information sued, and obtained compensatory damages of about $7,500. The judge refuesed to award punitive damages. An appeal is pending. *See* Jane Kirtley, *Committing Fraud to Protect Privacy?* American Journalism Rev., March 1999, at 70, available at **Error! Reference source not found.** (last checked March 25, 1999).

[31] Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 10 (1997).

[32] Jeffrey Rothfeder, *Privacy for Sale* 90 (1992).

and sellers of "high-ticket gifts."[33]

The combining of consumer information from a number of sources to create a more complete picture of a consumer's habits--called profiling--has become common.[34] One company, for example, "often can determine whether you own a dog or a cat, enjoy camping or gourmet cooking, read the Bible or lots of other books. It often can pinpoint your occupations, the car you drive, your favorite vacations. . . . [I]t often projects for its customers who should be offered a credit card or who is likely to buy a personal computer."[35]

Other notable stories abound. A company secured lists of consumers and their prescription medications from pharmacies and then sent the consumers reminders to refill their prescriptions or solicitations to switch to competing drugs, communications which were at least partly financed by drug manufacturers.[36] One company maintains a "birthday bank" containing

---

[33] Michael W. Miller, *Firms Peddle Information From Driver's Licenses*, Wall St. J., Nov. 25, 1991 at B1. *See also* Erik Larson, *The Naked Consumer* 134-36 (1992) (describing similar marketing techniques).

[34] *See generally* Roger Clarke, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance,* 4 J. L. & Information Science 403 (1993). For examples, *see, e.g.*, Daniel Mendel-Black & Evelyn Richards, *Peering into Private Lives*, Wash. Post, Jan. 20, 1991, at H1, H6:

> Vacuumed into huge databases around the country is information about how many times you went out to eat last month, about whether you dog prefers Alpo to Purina . . . . Details like these are sorted, digested and compiled so that computers can plop you into neatly defined categories to help determine the likelihood that you'll pay your Visa bill on time or buy a new brand of detergent or cigarettes within the next few months . . . .cashing in a coupon [can put your name and address on a list because] some that arrive at your home are encoded with digits that will identify you when you trade them in.

What Price Privacy? Consumer Reports 356 (May 1991):

> By overlaying the data available through thousands of information systems, it's now possible to create a remarkably detailed picture of anyone. That picture could include your age, income, political party, marital status, the number of children you have, the magazines you read, your employment history, and your military and school records. A data base might also know what kind of breakfast cereal you eat, the make of car you drive, even the brand of diapers your baby wears.

See also Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 Tex. L. Rev. 1395, 1400 (1987).

[35] Robert O'Harrow, Jr. *Are Data Firms Getting Too Personal?* Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy/8.htm> (last checked June 15, 1998).

[36] Evan Hendricks, *Class-Action Suit Targets CVS Over Use of Prescription Data*, Privacy Times, Apr. 3, 1998 at 1, 2. *See also* Evan Hendricks, *Rising Traffic in Prescription Info Causes Backlash in D.C.*, Privacy Times, Feb. 20, 1998, at 1, 2 (noting that efforts to market anti-depressants and schizophrenia drugs to mental health

the birthdays of some fifty million people. Retailers use the birthdays to target those who are celebrating turning points--eighteen, thirty, or forty, for example--and so might splurge.[37] The same company also maintains records on consumer heights and weights, information of interest to clothing sellers.[38]

Even the manner in which databases are created has raised questions. Richard S. Murphy has written that "the typical transaction between a merchant or seller and a consumer increasingly can be characterized as an exchange of goods or services for money *and information*."[39] But the information-gathering goes well beyond conventional transactions. A toy manufacturer reportedly ran a television commercial in which a clown asked children to place telephone handsets next to their TV's. The commercial then played tones which dialed an 800 number. A mechanism automatically recorded the telephone number of phones from which calls to the 800 number were placed.[40] The manufacturer then obtained the names and addresses which matched up to the telephone numbers, and it had a mailing list.

Adults are hardly immune from such tricks: in 1993 a manufacturer of a product for incontinent women established an 800 number for people who wanted free samples. It then offered for sale the list of the 4.4 million people who responded.[41] One woman began receiving

---

patients is "particularly controversial because of the greater potential for manipulation."); Center for Public Integrity, *Nothing Sacred* 27 (1998) (after woman visited doctor for routine tests, she received letter from "pharmaceutical company that had obtained access to her medical data and wanted her to try its new cholesterol medication."); Sheryl Gay Stolberg, *The Numbering of America: Medical ID's and Privacy (Or What's Left of It)*, NY Times, July 26, 1998, § 4 at 3.

[37] Jeffrey Rothfeder, *Privacy for Sale* 91-92 (1992).

[38] Jeffrey Rothfeder, *Privacy for Sale* 92 (1992).

[39] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Property*, 84 Georgetown. L. J. 2381, 2402 (1996) (italics in original).

[40] Gary T. Marx, *Privacy & Technology*, Whole Earth Rev., Winter 1991 at 90, 91. *See also* Daniel Mendel-Black & Evelyn Richards, *Peering into Private Lives*, Wash. Post, Jan. 20, 1991, at H1, H6 ("dialing an 800 number can put your name and address on a list."); Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy*, 12 J. Public Pol. & Marketing 106, 110 (1993) (describing technology that allows subscribers to toll-free numbers to obtain lists of callers' numbers).

[41] Kevin DeMarrais, *Big Brother is Watching Your Database*, The Record, Apr. 30, 1995 at A01. *See also*

solicitations directed to lesbians after she spent a night at a lodge. She later learned that the lodge catered primarily to lesbians, and had sold her name to a lesbian mailing list.[42]

Similarly, the Federal Trade Commission has determined that businesses operating websites collect a great deal of information from consumers, including children, often without disclosing to consumers how the information will be used.[43] Ninety-two percent of the websites in one sample collected personal information, including such data as social security numbers, gender, and age.[44] Only fourteen percent of the sites disclosed their information practices.[45] Nearly ninety percent of the websites directed at children collect personal information, [46] To gather information from children like names, mail addresses, phone numbers, ages, gender, hobbies, and interests, websites have imaginary characters pose questions, have children sign a guest book, solicit information to create home pages for children, invite children to join chat and

---

Jeffrey Rothfeder, *Privacy for Sale* 92-93 (1992) (similar lists created from consumers who called toll-free numbers to find out pollen count by zip code--who later received solicitations from sellers of antihistamines--and consumers who called to receive Thanksgiving turkey cooking tips--who subsequently were sent mailings from poultry farms); Evan Hendricks, *Rising Traffic in Prescription Info Causes Backlash in D.C.*, Privacy Times, Feb. 20, 1998 at 1, 3 (drug companies said to capture phone numbers from consumers calling toll-free numbers for various medications); Evan Hendricks, *Companies Exploiting Internet's Ability to Track Consumer Habits*, Privacy Times, July 3, 1995, at 3, 4 (company which runs "Free Offer Outlet" on computer services harvests names, addresses, and phone numbers of people who accept free offers and provides information to sponsors for market research and follow-up; harvesting from one computer service alone said to generate over 300,000 leads in four months). Western Union advertised a similar practice to debt collectors with a debtor's address but not a phone number: the company offers to send to the debtor a letter stating that the debtor has a telegram waiting, and that if the debtor calls Western Union, the debtor can obtain the telegram. When the consumer calls, Western Union is able to obtain the telephone number from which the debtor is calling. The Court of Appeals for the Ninth Circuit has ruled that this practice amounts to debt collection and so Western Union must comply with the Fair Debt Collection Practice Act, 15 U.S.C. § 1692 et seq. Romine v. Diversified Collection Services, Inc., ___ F.3d ___, No. 97-15586, 1998 U.S. App. Lexis 22606 (9/17/98).

[42] Larry Tye, *List-makers Draw a Bead on Many*, Boston Globe, Sept. 6. 1993 at 1.

[43] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 22, 27 (1998).

[44] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 23, 25 (1998). The FTC took a number of different samples of websites, the largest of which it labeled the Comprehensive Sample. Other samples included a Retail Sample, Financial Sample, Children's Sample, and Most Popular Sample. Unless otherwise indicated, information reported in this article will relate solely to the Comprehensive Sample.

[45] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 27, (1998). *But see* Claire Coyne, *DMA Scan Shows Most Web Sites Post Privacy Policies*, DMA News, June 15, 1998, avaliable at <http://www.the-dma.org/texis/scripts/news> (last checked Nov. 12, 1998) (DMA review of web sites shows that most post privacy policies).

[46] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 31 (1998).

electronic pen pal programs, require children to register with the site, or offer prizes and other incentives for providing information.[47] The FTC also found that "numerous sites" either sell children's personal information to others, or simply post it online, including some sites that post color pictures of children with their full names and ages.[48]

Stories like these--involving conflicting desires for privacy and for information which may be of some value--have become commonplace.[49] Privacy, of course, means various things to various people.[50] In this paper, I am concerned only with what has been called by some, informational privacy,[51] and, by others, confidentiality or data protection;[52] that is, any rights an individual has or should have to prevent businesses and individuals from obtaining, using, and selling information concerning the individual, and conversely, the rights businesses and individuals should have to use that information without the knowledge or consent of the individual to whom the information pertains.

The laws regulating personal information--especially information contained in

---

[47] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 32, 33 (1998); *see also* Shelley Pasnik & Mary Ellen R. Fise, *Children's Privacy and the GII*, in National Telecommunications and Information Administration, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>.

[48] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 36-37 (1998).

[49] As Arthur R. Miller put it, "At bottom, one person's 'I want to know' conflicts with another's 'leave me alone.'" Arthur R. Miller, *The Right of Privacy--A Look Through the Kaleidoscope*, 46 SMU L.Rev. 37, 38 (1992).

[50] *See, e.g.*, Charles Fried, *Privacy: Economics and Ethics; A Comment on Posner*, 12 Ga. L. Rev. 423, 423 (1978) ("privacy is to be defined as the control of information about oneself."); Charles Fried, *Privacy*, 77 Yale. L. J. 475, 493 (1968); Alan F. Westin, *Consumer Privacy Issues in the Nineties* in Louis Harris & Associates & Alan F. Westin, *The Equifax Report on Consumers in the Information Age* xviii (1990) (hereinafter, 1990 Equifax Report) ("privacy is the claim of individuals to decide what information about themselves will be communicated to others."); Jeffrey H. Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 Computer & High Tech. L.J. 27, 30 (1995) ("privacy is the condition in which others are deprived of access to you."); John T. Soma & Richard A Wehmhoefer, *A Legal and Technical Assessment of the Effect of Computers on Privacy*, 60 Denver L. J. 449, 450 (1983) (privacy is "the unitary concept of separation of self from society."); Fred H. Cate, *Privacy in the Information Age* 19-31 (1997) (canvassing definitions).

[51] *See, e.g.*, Jacob Sullum, *For Sale*, Reason, Apr. 1992, at 29 ("the amorphous concept of informational privacy, variously described as a right, a concern, an interest, and a preference.").

[52] *See, e.g.*, Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Public Pol. & Marketing 149, 149 (1991).

computerized databases--are a patchwork of *ad hoc* responses to outrage over past invasions of privacy, rather than a coherent set of rules based on underlying principles and policies. [53] Some information cannot be sold, while other information is somewhat regulated, and most personal information is not regulated at all. [54] For example, suppose a bookstore, and a videotape rental store, realizing that people often wish to see videos based on the books they have read, desired to enter into an agreement: the bookstore would tell the video store which of its customers had purchased books which had been made into videos--so that the video store could solicit the customers to rent the videos--and the video store would provide the bookstore with the names of customers who had rented videos based on books. At present, federal law prohibits video rental stores from knowingly disclosing the names of movies rented by their customers, but nothing

---

[53] Among the privacy statutes regulating commerce (as distinct from statutes governing data held by government) are the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (governing credit reports and similar reports on consumers), the Family Educational Rights and Privacy Act (the so-called "Buckley Amendment"), 20 U.S.C. § 1232g (regulating information provided by educational institutions), the Right to Financial Privacy Act, 12 U.S.C. §1101 et seq. (bank records), the Cable Communications Policy Act, 47 U.S.C. § 551(a) (cable television), the Employee Polygraph Protection Act, 29 U.S.C. § 2001-09 (limiting employers' ability to use lie detectors), the Video Privacy Protection Act, 18 U.S.C. §§ 2710-11 (barring video stores from disclosing information), and the Telemarketing Protections Act, 47 U.S.C. § 227 (limiting the use of automatic dialing machines in telemarketing). *See* Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 Computer & High Technology L. J. 151, 170-71 (1995):

> Legal conceptions of privacy are notoriously uncertain. Within the universe of legal concepts, privacy laws often seem to behave like the fractals in chaos theory - ever-changing in unpredictable but patterned ways. Some years ago, Chief Justice Rehnquist described the privacy cases decided by the United States Supreme Court as "defying categorical description." Professor Arthur R. Miller chose "A Thing of Threads and Patches" as the title of one of the chapters in his influential book, *The Assault on Privacy*. A federal judge once described privacy law as like a "haystack in a hurricane. Privacy laws seem to have this amorphous quality in part because privacy depends to some extent on each person's expectations regarding respect for her individual personality.

See also Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 Fed. Com. L.J. 195, 209-10 (1992) (footnote omitted):

> Existing federal legislation only addresses privacy concerns in particular industry contexts. Although each of these industry-specific laws contains detailed obligations, they provide a sphere of protection to isolated concerns for narrowly-identified problems and are incomplete responses to information privacy issues.

Professor Reidenberg reviews various privacy laws at *id.*, pp 210-36.

[54] For example, cable television operators cannot disclose what shows their viewers have watched on pay-per-view. See 47 U.S.C. § 551. The disclosure of credit reports is regulated so that only those who wish to see them for certain purposes may do so. *See* 15 U.S.C. § 1681b.

prevents bookstores from revealing the names and purchases of their patrons. [55] Similarly, if the consumer paid with a credit card, no federal law would bar the credit card issuer from disclosing that the consumer had done so.[56] These inconsistencies, as well as others, make little sense. [57]

Legal scholars and others have responded to this privacy bramble bush in a number of ways. Some have brought to bear the analyses of law and economics.[58] Others have analyzed the problems created under traditional privacy doctrines or suggested rules to regulate data collection.[59] Some have articulated broad principles intended to govern data collection, often focusing exclusively or largely on fairness considerations. [60] And some have discussed the impact of foreign laws--chiefly the European Directive on Data Privacy--on data collection in the United States.[61] But few have explored the ways consumers behave or the insights which inform other laws governing consumer-merchant transactions. My purpose in this article is to bring to bear on

---

[55] *See* 18 U.S.C. § 2710. Or as Vice President Al Gore has said: "We live in a nation where people can get access to your bank account and your medical records more easily that they can find out what movies you rent at a video store." *See* Sheryl Gay Stolberg, *Privacy Concerns Delay Medical ID's*, NY Times, Aug. 1, 1998, at A10.

[56] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 270 (1996). Some states do regulate disclosures by credit card issuers. Thus, Virginia bars merchants from selling "any information gathered solely as the result of any customer payment by . . . credit card . . . ." Va. Code § 59.1-442, while California requires credit card issuers to allow credit card holders to opt out of the disclosure of their information. Cal. Civ. Code § 1748.12. *See infra* note ___.

[57] Similarly, your cable television company may not lawfully communicate to others what channels you watch, 47 U.S.C. § 551, but nothing prevent your local movie house from announcing your viewership. Indeed, it is debatable whether federal law prohibits wireless cable service operators or direct broadcast satellite systems operators from disclosing viewing habits. *See* U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 16-17 (1995).

[58] *See, e.g.*, Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393 (1978); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Georgetown L. J. 2381 (1996).

[59] *See, e.g.*, Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 Fed. Comm. L. J. 195 (1992); Reidenberg, *Setting Standards*; Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 Computer & High Tech. L. J. 431 (1993).

[60] *See, e.g.*, Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* 6-7 (1995) (users of information should disclose uses of information).

[61] *See, e.g.*, Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 Vill. L. Rev. 129 (1996); P. Amy Monahan, *Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses*, 29 Law & Pol. In Int'l Bus. 275 (1998). For a thorough discussion of the extent to which United States laws meet European standards, see Paul M.

privacy issues some principles and policies drawn from existing consumer regulation and, to some extent, the literature on consumer behavior and consumer transactions. In so doing I hope to contribute to the formation of doctrine regarding privacy and the trade in personal information.

Part II of this article discusses the benefits from the sale of personal information. In Part III, I turn to the taste for privacy--why do people care about privacy, and how much they care. Those who are already knowledgeable about the trade in personal information and privacy might do well to skip those parts. Part IV explores the conflicts between what people say and what they do; more specifically, if people say they care about privacy, and in some circumstances act to protect their privacy, why do so few consumers opt out of marketing solicitations? I argue in Part IV that marketers have both incentives and the ability to increase consumers' transaction costs in protecting their privacy; that some, perhaps many, marketers do in fact inflate the transaction costs incurred by consumers; and that many consumers, faced with significant transaction costs and certain constraints common to consumers, decide not to protect their privacy. In Part V, I suggest ways to reduce consumer transaction costs in protecting informational privacy.

II. The Benefits from the Trade in Information

A. Information Seekers

1. Commercial Interests

Though consumer information is employed for far too many purposes to catalog here, some understanding can be attained by mentioning two uses. The first involves situations in which a consumer seeks some benefit. For example, reports on consumers may be used when a person applies for a loan, employment, insurance, or even to rent a home.

Schwartz & Joel R. Reidenberg, *Data Privacy Law* (1996).

A second use of information--marketing--differs significantly from consumer-initiated transactions. When a consumer applies for something, the merchant may desire information to decide whether to grant the consumer's request. When computers are used for marketing, however, the merchant seeks the information--generally without the consumer's knowledge--as part of the merchant's own sales process.[62] Though the consumer may ultimately accept the vendor's offer, it is the merchant, not the consumer, who starts the process by seeking information about the consumer (or, more accurately, to ask the questions to which the consumer's name is one answer).

The use of computer databases for marketing may take various forms. In one form, businesses sell their customer lists to other companies, typically so that the purchasing business may solicit additional consumers. [63] List sellers find such sales highly remunerative because there are few additional costs in selling a list that the seller already may maintain for other purposes. [64] Indeed, with profit margins of up to sixty percent, some businesses reportedly earn more from selling customer lists than from selling the goods which prompted the consumers to land on their customer lists.[65] Companies have even been pursued by merger partners because of their lists. [66]

Another form of marketing is called prescreening. A lender who wishes to solicit a large number of people for credit cards might ask a credit bureau to identify people who meet criteria

---

[62] As one commentator put it, the merchant wishes "to maximize the future streams of revenue from sales while minimizing the future sum of expenses related to producing those sales. Gathering information about the tastes, preferences, and responsiveness of consumers to monetary and other incentives is believed to be critical to the realization of these goals." Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. Chi. Legal Forum 77, 88.

[63] Some publications provide their list to others as often as 52 times a year. Karlene Lukowitz, *Cashing in on Renting Your List*, Folio, Oct. 1985, at 106.

[64] *See* Karlene Lukowitz, *Cashing in on Renting Your List*, Folio, Oct. 1985, at 106 (quoting list-manager as saying "List rentals are almost all gravy.").

[65] Susan Headden, *The Junk Mail Deluge*, U.S. News & World Rep., Dec. 8, 1997; Jill Smolowe, *Read This ! ! ! ! ! ! ! !* Time, Nov. 26, 1990 at 62.

[66] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 336-37 (1996) (pharmaceutical company merged with mail order pharmacy to obtain latter's detailed records; prescription drug benefits plan manager sought to buy corporation that maintained prescription drug database and owned pharmacies).

specified by the lender, such as a past record of paying bills when due and a certain income level. Under this prescreening process, the credit bureau supplies the lender or its agent with the names of those who meet the criteria, or might mail the solicitation directly. The lender never sees the names of those who do not meet its criteria. Those who pass the test know only that they have received the mailing; those who do not satisfy the criteria typically never even know that they were considered unfit for an offer made to others.[67]

Some businesses use computers for sophisticated marketing ventures. Thus, supermarkets are able to gather information about their customers through electronic scanners, applications for check-cashing and preferred-shopper cards, shopper surveys, and the like. Armed with this data, supermarkets can mail cat-owners coupons for kitty litter and offer discounts on diapers to those with small children. [68] The supermarket can even encode the coupons to determine which people responded to which coupons, information which may be useful in future marketing attempts. [69] A number of major corporations are reported to monitor consumer purchases both to bombard consumers with solicitations and to sell the information to

---

[67] *See generally* Sheldon Feldman, *The Current Status of the Law Governing Prescreening, Including Permissible Postscreening Practices*, 46 Bus. Law. 1113 (1991). Pre-screening is now regulated by the Fair Credit Reporting Act, which permits pre-screening subject to certain safeguards, and requires consumer reporting agencies to allow consumers to have their names removed from lists maintained for pre-screening. *See* 15 U.S.C. §§ 1681b(e), 1681m(d).

[68] *See The Supermarket as Selling Machine*, 58 Consumer Reports 560, 560 (1993).

[69] *See* Gary T. Marx, *Privacy & Technology*, Whole Earth Rev., Winter 1991, at 90, 91-92; Daniel Mendel-Black & Evelyn Richards, *Peering into Private Lives*, Washington Post, Jan. 20, 1991, at H1, H6. Mendel-Black and Richards also describe the following:

> Sharper Image. . . . keeps one list of its own 800,00 mail-order buyers and another of 1.2 million people who have shopped at its retail stores. Every 18 months, the company learns considerably more about who these people are by supplying the names to National Demographics & Lifestyles, a Denver outfit with detailed characterizations of 30 million people gleaned from product registration forms returned by buyers. National Demographics matches Sharper Image's customers against names in its own database, then concocts a statistical description. The most recent finding was something like this: The typical Sharper Image buyer is male, between the ages of 45 and 55, with a household income of $70,000. National Demographics then reaches into its database and supplies the retailer with the names of thousands more Americans who fit that description.

others.[70]

These various marketing endeavors are far from insignificant to business. A 1996 Gallup poll found that 77% of commercial firms use direct marketing. [71] The total amount spent on mailing lists alone--without taking into account the sales of good and services they generate--is said to run $3 billion a year. [72] According to one estimate, direct-marketing-generated electronic commerce could exceed $4 billion in 1998, and rise to $30 billion by 2002. [73] The direct marketing industry reportedly employs more than eighteen million people. [74] And the business is growing, at a rate estimated at twice that of the United State' gross national product. [75]

2. Non-commercial Interests

One reason-- already alluded to--that people search for facts about someone else is simple curiosity: has my professor received a speeding ticket; what can I find out about the person my child is dating, or my ex-spouse; and the like. [76] But consumers seek access to data for other

---

[70] *See, e.g.*, Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issue*, 12 J. Public Pol. & Marketing 106, 110 (1993) ("Major corporations analyzing and/or renting out purchase information include American Express, Blockbuster Entertainment, Lotus, McDonald's, and Philip Morris. . . ."); John Markoff, *American Express Goes High-Tech*, NY Times, July 31, 1988, § 3 at p.1.

[71] Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 7 (1997).

[72] William J. French, *Common Law Protection of Individuals' Rights in Personal Information*, 65 Fordham L. Rev. 951, 956 (1996).

[73]Hearings before the H. Com. on Commerce, Subcomm. on Telecommunication, Trade, & Consumer Protection, *Protecting Consumers Against Cramming and Spamming* (Sept. 28, 1998) (Testimony of Jerry Cerasale, Senior Vice President, Direct Marketing Association), available at <http://com-notes.house.gov/cchear> (last checked Oct. 16, 1998).

[74] William J. French, *Common Law Protection of Individuals' Rights in Personal Information*, 65 Fordham L. Rev. 951, 956 (1996).

[75] Arthur M. Hughes, *The Complete Database Marketer* 4 (1991) ("It is and will continue to be the hottest growth area in advertising for the foreseeable future.").

[76] *See, e.g.*, Yohay v. City of Alexandria Employees Credit Union, 827 F.2d 967 (4th Cir. 1987) (person obtained credit report on ex-spouse); Jones v. Federated Financial Reserve Corp., 144 F.3d 961 (6th Cir. 1998) (person obtained credit report on roommate's ex-spouse); Gini Graham Scott, *Mind Your Own Business* 325 (1995) ("people check up on neighbors, friends, dates, mates, family members, and others."); Rajiv Chandrasekaran, *Doors Fling Open to Public Records*, Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy9.htm> (last checked June 15, 1998) (college students using Lexis-Nexis to check on dates' ages and marital status); Privacy Rights Clearinghouse, S *econd Annual Report of the Privacy Rights Clearinghouse* 40-41 (1995) (parents checking on son's fiancee)

reasons too, and some of these are easier to justify. Information services have helped find abducted children and so-called deadbeat dads.[77] Or a spouse might disappear, leaving the remaining spouse with debts incurred jointly.[78] Some have found long-lost relatives, important witnesses in litigation, or others who were important to them through internet services.[79]

On the other hand, some use computers as an adjunct to an unlawful act, such as stalking.[80] Abusive spouses have been known to hunt fleeing partners on the internet, and criminals have employed the internet to steal identities.[81] Obviously, such uses can be a serious problem and an individual's desire to use computers in such ways should not be indulged under any circumstances.

B. Consumers

Consumers may also benefit from having their names appear in databases. Indeed, some are so persuaded of these benefits that, as discussed below, they are willing to pay for the privilege.[82] What advantages might consumers receive by appearing in databases? First, many

---

[77] Public Workshop on Consumer Information Privacy, Session One: Database Study, at 229 (June 10, 1997) available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Bruce Hulme, Special Investigations, Inc., Legislative Committee Member, National Council of Investigation and Security Services) (service recovered over 2,000 abducted children); Statement of Geraldine Jensen, President, Association for Children for Enforcement of Support, Inc., to FTC, available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments1/aces2.htm> (last checked Aug. 21, 1998) (service has assisted over 25,000 families in locating absent parents who owe child support; average family collected $4,000 per year in child support, enabling 88% of clients on welfare to become self-sufficient when child support payments were joined with available earned income).

[78] Jeffrey Rothfeder describes such an incident in *Privacy for Sale* at 106-22 (1992).

[79] For examples, see the stories collected at <http//www.switchboard.com/stories.htm> (visited Aug. 4, 1998). *See also* FTC, Public Workshop on Consumer Information Privacy, Session One: Database Study, at 6 (June 10, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (Remarks of Chairman Pitofsky) ("databases have been critical in locating witnesses, tracking down criminals, and even reuniting lost family members); Rajiv Chandrasekaran, *Doors Fling Open to Public Records*, Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy9.htm> (last checked June 15, 1998).

[80] For a chilling account of the role of computers in the stalking and eventual murder of actress Rebecca Schaeffer, see Jeffrey Rothfeder, *Privacy for Sale* 13-15 (1992).

[81] Center for Public Integrity, *Nothing Sacred* 7 (1998).

[82] See *infra* note ___ and accompanying text.

make purchases through direct marketing channels. [83] More than half the respondents to a 1996 Equifax survey say they or someone in their household had bought something from a mailing in the year preceding the survey. [84] Fourteen percent of the respondents to a 1990 survey had purchased something offered to them in a telephone call. [85] Indeed, consumers responding to direct marketing reportedly bought nearly $600 billion worth of goods and services in 1995. [86]

Second, consumers whose interests are correctly identified by sellers may reduce their search costs.[87] For example, a consumer who wishes to purchase a new computer might be grateful to receive an unsolicited computer catalog in the mail because it could save the consumer a trip to a computer store.

Third, some claim that the greater availability of information actually reduces junk mail. The more sellers learn about consumers, the argument goes, the better they can target mailings, and thus avoid sending solicitations to those who do not want them. [88] If businesses are deprived of consumer information, some say, they will respond by soliciting all consumers, not just the ones most likely to be interested in their product. [89] Response rates to mailings have risen in

---

[83] Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 Harv. J. L. & Pub. Pol. 591, 599 (1994) ("Many consumers enjoy receiving mailings and shopping at home.").

[84] *See 1996 Equifax/Harris Consumer Privacy Survey* at 18. *See also 1990 Equifax Report supra*, note ___, at 68 (same, and sixteen percent had made such purchases more than five times); *Learning Where to Draw the Line on Privacy Issue*, Advertising Age, Feb. 15, 1993, at 35 (quoting DMA representative that over 100 million Americans had shopped at home in some form in previous year.)

[85] *See 1990 Equifax Report supra*, note ___, at 68.

[86] Private Ayes, Marketing Tools, Jan.-Feb. 1996 at 31. This number is projected to grow at a rate of 7.2 % a year. Neil Munro, *Putting a Price on Technology*, 11 Wash. Technology, No. 23, Mar. 6, 1997.

[87] *See* Daniel Klein & Jason Richner, *In Defense of that Pesky Junk Mail*, Chicago Tribune, Apr. 20, 1992 at 19 ("Direct mail is especially important for customers who do not live in a major metropolitan area, or who have a physical or health disability that makes shopping and travel difficult."); Anthony T. Kronman, *The Privacy Exemption to the Freedom of Information Act*, 9 J. Legal Studies 727, 747 (1980).

[88] The argument is presented and criticized in Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1217-18 (1998). Kang argues that if less privacy actually benefited consumers by reducing their junk mail, consumers would choose to surrender their privacy.

[89] Those who market through e-mail have been known to adopt such a strategy anyway. One e-mail marketer has reportedly stated "It's just as cost-effective for me to send to six million e-mail addresses as one million, so why bother?" *See* Dee Pridgen, *How Will Consumers be Protected on the Information Superhighway?* 32 Land & Water L. Rev. 237, 240 (1997). *Cf.* FTC, Public Workshop on Consumer Information Privacy, Session

recent years, suggesting that direct marketers have improved their ability to identify likely buyers.[90]

But the argument is flawed. Even if response rates have risen to five percent, that still means that 95% of the recipients of an offer are not interested in it--and, as discussed below, many in that 95% would rather not have received the offer. [91] Indeed the costs of nonconsensual databases--in terms of unread mailings and unwanted telephone solicitations--is estimated to approach $50 billion annually. [92] The argument also assumes that businesses would not respond to the loss of information by abandoning direct mail, in favor of other marketing mechanisms, which might become comparatively cheaper than sending mail to many more consumers. Finally, the argument presupposes that systems to reduce junk mail in other ways cannot be devised.

Fourth, consumers who wish to borrow and who maintain good credit records benefit from lender access to their records; if lenders could not determine that a particular consumer was credit-worthy, they might charge the consumer higher interest rates, to compensate them for the risk they were taking in lending to a person with no credit history, or refuse to lend to the consumer at all. [93]

Fifth, some products which some consumers want might not be available but for

---

Three: Consumer OnLine Privacy, at 13 (June 12, 1997) available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Jason Catlett, CEO, Junkbusters Corp.) (10,000 pieces of spam cost a dollar to send).

[90] Richard Lacayo, *Nowhere to Hide*, Time, Nov. 11, 1991 at 34; Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues*, 12 J. Public Pol. & Marketing 106, 108 (1993).

[91] Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues*, 12 J. Pub. Pol. & Mktg. 106, 108 (1993). Response rates to telemarketing are said to be even higher than for direct mail. Caroline E. Mayer, *Telemarketers Answering Their Calling,* Wash. Post, August 31, 1997 at H1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/sidebars/phone/10.htm> (last checked June 15, 1998).

[92] Kenneth C. Laudon, *Markets and Privacy*, 39 Communications of the ACM No. 9 (Sept. 1, 1996).

[93] *See* Judith Beth Prowda, *Privacy and Security of Data*, 64 Fordham L. Rev. 738, 751 (1995).

computer databases. These databases furnish names needed for marketing research, and in the absence of such research, some sellers might decide against taking on the risk and expense of introducing certain new products. [94]

Sixth, the use of computer databases in marketing also makes it possible, at least theoretically, to sell products at lower cost.[95] Sellers use databases to assist them in selling goods when they believe that the cost of that use, per sale, is cheaper than other marketing mechanisms. The average return for a dollar spent on direct mail advertising is ten dollars, more than twice the return for a dollar spent on television commercials. [96] The average mailing generates ten times the response produced by a newspaper ad and 100 times the response from a television commercial. [97] Hence, more money is spent on direct mail than on magazine ads, radio commercials, or television pitches. [98] If sellers were denied access to databases as marketing mechanisms, they would either be forced to employ more expensive selling methods--measured by the cost per sale--or else forgo selling the product altogether, if alternative methods were too costly to make selling the item profitable. [99] If the cost per sale increases, probably the sale price

---

[94] *See* Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Public Pol. & Marketing 149, 159 (1991) ("Since marketing research remains essential to carrying out the marketing concept--developing products and services that meet consumer needs--some intrusion may be necessary to conduct accurate marketing research. For example, obtaining a random sample may require telephone or personal contact with a number of people who are not interested in the product under consideration. If marketing research costs increase substantially due to privacy regulation, all consumers may experience price increases, when in fact only a limited number of people may be concerned about privacy."). Some have urged dealing with this problem by having different rules for marketing research than for conventional marketing. *See* Robert E. Shaw, *Telemarketing: Its Impact on the Research Industry in the United States*, European Research 78 (May 1987).

[95] *See, e.g.*, David J. Klein, Note, *Keeping Business Out of the Bedroom: Protecting Personal Privacy Interests from the Retail World*, 15 J. Computer & Info. L. 391, 393, n.10 ("Some companies can offer discounts on their goods when they utilize personality profile lists, because they send fewer mail advertisements, and they send them only to those persons who are likely to purchase the product.").

[96] Susan Headden, *The Junk Mail Deluge*, U.S. News & World Rep., Dec. 8, 1997.

[97] Jill Smolowe, *Read This ! ! ! ! ! ! ! !* Time, Nov. 26, 1990 at 62.

[98] Jill Smolowe, *Read This ! ! ! ! ! ! ! !* Time, Nov. 26, 1990 at 62.

[99] *Cf.* Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Public Pol. & Marketing 149, 159 (1991). ("small business owners in Alaska claimed they need access to tourism mailing lists to carry out successful promotion and promote entrepreneurial development . . . . "); *What Price Privacy?* Consumer Reports 356, 359

of the product will also increase. Consequently, those who do wish to buy the product will pay a higher price for it, in essence paying to protect the privacy of another.

Seventh, some claim that mail-order selling reduces damage to the environment because it enables people to shop without traveling.[100]

In sum, the use of computer databases to maintain information on consumers benefits many.[101] Some claim that because businesses have a stake in the outcome of discussions on privacy, they inflate the benefits generated by databases and underestimate the costs they produce.[102] That is a credible argument. But it seems clear that some value the trade in personal information, even if the benefits are somewhat exaggerated. The next section looks at a cost of that trade--its effect on privacy.

III. The Taste for Privacy

A. Why Do People Care About Privacy?

In a number of articles Judge (then-professor) Posner attempted to construct an economic theory of the right to privacy.[103] Posner focused on privacy as an intermediate goal, because, he wrote, regarding privacy purely as a consumption good "would bring the economic analysis to a

---

(May 1991) ("The direct mail chief at one of the nation's largest catalog houses says that by using more sophisticated mailing lists, his company has been able to cut its annual mailings by 25 percent and increase the response rate too. 'For us,' he says, 'that spells the difference between making a solid profit or closing our doors.'").

[100] Judith Beth Prowda, *Privacy and Security of Data*, 64 Fordham L. Rev. 738, 751 (1995); Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 Harv. J. L. & Pub. Pol. 591, 600 (1994); Daniel Klein & Jason Richner, *In Defense of that Pesky Junk Mail*, Chicago Tribune, Apr. 20, 1992 at 19. *But see infra* notes ___ and accompanying text reporting arguments that direct mail solicitations damage the environment.

[101] *See also* Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Public Pol. & Marketing 149, 159 (1991) ("Protection of consumer privacy may inadvertently harm other segments of society. . . . Also, telemarketers create jobs and shopping opportunities for the handicapped . . . , as well as development of depressed rural areas. . . .").

[102] *See* Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues*, 12 J. Pub. Pol. & Mktg. 106, 108 (1993).

[103] *See* Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393 (1978); Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 Buffalo L. Rev. 1 (1979); Richard A. Posner, *An Economic Theory of Privacy*, Regulation 19 (May/June 1978). The first of these pieces was commented on by a variety of scholars in the same issue of the Georgia Law Review. A series of papers applying a law and economics approach to the right to privacy

grinding halt because tastes are unanalyzable from an economic standpoint." [104] Judge Posner viewed the demand for privacy as stemming largely from a desire to conceal either "discreditable information"--that is, "information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards"--or information which would "correct misapprehensions that the individual is trying to exploit; [105] a would-be borrower, for example, might wish to conceal from lenders the fact that she has previously defaulted on a loan.

Many consumers, however, seem to reject this view of privacy. One survey found that sixty-four percent disagreed with the statement "most people who complain about their privacy are engaged in immoral or illegal conduct." [106] Perhaps viewing privacy as an end in itself, rather than as a means to an end, retards analysis in some respects, but an economic theory which overlooks the reality that for some privacy has value as an end is necessarily incomplete. [107]

What is behind the "taste for privacy"? Alan F. Westin has speculated that it may be biological in origin. [108] Some commentators have suggested that privacy is so fundamental to life that few pleasures can survive without it. [109] The available psychological literature, though

---

also appears at 9 J. Legal Stud. 621-842 (1980), with a brief introduction by Judge Posner.

[104] *See* Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 394 (1978).

[105] *See* Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 399 (1978). In a later piece, Judge Posner wrote that the desire to protect against embarassment also motivates privacy, and is more worthy of legal protection. *See* Richard A. Posner, *Privacy*, in 3 *The New Palgrave Dictionary of Economics and the Law* 103, 105 (1998).

[106] Priscilla M. Regan, *Legislating Privacy* 48 (1995).

[107] *See* Edward J. Bloustein, *Privacy is Dear at Any Price: A Response to Professor Posner's Economic Theory*, 12 Ga. L. Rev. 429, 442 (1978) ("It may be that Posner's fundamental error arises out of his attempt to distinguish privacy as an `instrumental' value from privacy as a `final' value. . . .privacy is so integrally and inextricably related to the maintenance of personal dignity, an `ultimate' or `final' social value of extraordinary importance, that the law must also protect privacy . . . ."); Anthony D'Amato, *Comment: Professor Posner's Lecture on Privacy*, 12 Ga. L. Rev. 497, 499 (1978).

[108] *See* Alan F. Westin, *Privacy and Freedom* 8-11 (1967).

[109] *See* Charles Fried, *Privacy*, 77 Yale L. J. 475, 477 (1968) (Privacy "is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. . . . without privacy they are simply impossible."). For a discussion of the philosophical underpinnings of privacy doctrine, see Priscilla M. Regan, *Legislating Privacy* 24-33 (1995).

sparse, suggests that the desire for privacy may have a number of motives. [110]

The feelings generated by privacy invasions can be deeply held. Arthur Miller has observed that "Some people feel emasculated when private information about them is disclosed or exchanged even though the data are accurate and they do not suffer any career or social damage."[111] For example, the incontinent women who wished free samples of a helpful product[112] may object to disclosure of their condition not because they are trying to conceal criminal or immoral conduct or because they wish to exploit the ignorance of others, but because they fear the feelings they will experience if others find out. [113] Joel Reidenberg has written that "the treatment of personal information is an element of basic human dignity. Fair treatment of personal information accords respect to an individual's personality." [114] In Richard S. Murphy's words, "in the utility calculus, these psychic benefits count." [115]

Some consumers with a taste for privacy may be concerned about the loss of control. For example, consumers engaged in transactions which appear limited in scope may in fact provide information used far beyond the particular transaction. A child who celebrates a birthday at an

---

[110] *See* Cathy Goodwin, *A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption,* 1 J. Consumer Psych. 261 (1992) ("Qualitative data suggest that consumers seek privacy to enhance the quality of the consumption experience, to avoid interference from disapproving reference groups, and to resolve cognitive discomfort associated with self-discrepancy.").

[111] Arthur R. Miller, *The Assault on Privacy* 48-49 (1971).

[112] See *supra* note ___ and accompanying text.

[113] *Cf.* U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 3 (1995) ("an individual may want to keep certain types of health data confidential from the general public because its disclosure could cause the person embarrassment.); Anthony T. Kronman, *The Privacy Exemption to the Freedom of Information Act,* 9 J. Legal Studies 727, 746-47 (1980) (footnotes omitted):

> Why are people ever embarrassed when their interests are revealed to others who share the same interests? Perhaps disclosure awakens feelings of shame or guilt: the other person's knowing wink is a reminder of what one wishes to forget. Alternatively, the disclosure of a sensitive fact about oneself, even to someone who happens to be sympathetic, may raise a fear that the same information will be revealed to others who are *not* sympathetic or approving.

[114] Reidenberg, *Setting Standards supra,* note ___ at 498. For discussion of the role of dignity in privacy, see Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 Stanford L. Rev. 1193, 1259-65 (1998).

[115] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Property,* 84 Georgetown. L. J. 2381, 2386 (1996).

ice cream store may unwittingly become an entry in a database. [116] Similarly, some people object to others knowing their income, or how much their home cost. [117] Consumers may also wish to keep information private to deny others access to still other information; for example, someone who knows your social security number and mother's maiden name may be able to learn your bank account balances. [118]

Some have very concrete reasons for protecting their privacy. For example, privacy can be a matter of personal safety for police officers who wish to conceal their home addresses from vengeful criminals. [119] Others are concerned about identity theft. [120]

Consumer objections to unwanted solicitations also have a number of bases. Some want merely to be let alone; who has not been annoyed by a telephone solicitation at dinnertime? Many find intrusions in the home particularly irritating--and consumer law has been especially responsive to this concern, often providing protections not available elsewhere to consumers solicited in their homes. [121]

Even the unwanted paper troubles: it has been estimated that the average professional in

---

[116] *See* Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Public Pol. & Marketing 149, 152 (1991).

[117] Hal R. Varian, *Economic Aspects of Personal Privacy*, in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>.

[118] U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 3 (1995). Another explanation offered for the importance of informational privacy is that withholding information from others makes it possible to attain greater intimacy with selected individuals by sharing secrets with them. *See* Charles Fried, *Privacy*, 77 Yale L. J. 475 (1968).

[119] Mark Lewyn, *You Can Run, But It's Tough to Hide from Marketers*, Bus. Week, Sept. 5, 1994 (family of police officer).

[120] *See* Edmund Mierzwinski, *Data Dealers Seizing Control of Our Lives*, 19 At Home With Consumers No. 1, at 4 (May 1998) ("unrestricted sale of credit headers is one of the main causes of financial identify theft . . . a growing crime that leaves up to 40,000 or more consumers each year fighting to clear their names and correct their credit reports after thieves establish fraudulent credit accounts in their names.").

[121] For example, the Federal Trade Commission has promulgated a regulation providing consumers solicited in the home a three-day cooling off period in which to rescind any purchases. *See* 16 C.F.R. Part 429. Some states have enacted similar statutes. *See, e.g.*, NY Per. Prop. L. § 425 *et. seq.* Some states have even enacted such statutes for telephone sales; a list appears in Dee Pridgen, *Consumer Credit and the Law* App. 15A (1994).

the United States will spend eight months sorting junk mail over the course of a lifetime. [122] Some consumers complain that mail they want to receive gets lost in the flood of junk mail. [123] Environmentalists have claimed that junk mail makes up three percent of the nation's landfills. [124] According to one estimate, the average American received 553 pieces of junk mail in 1997, totaling 4.5 million tons for the entire country. [125]

Some are concerned about the volume of commercial e-mail messages. America On-Line receives thousands of complaints about unsolicited commercial e-mail every day [126]--making it by far the most frequent subject of complaint by AOL subscribers. [127] Depending on the day of the week, between five percent and thirty percent of the e-mail received by AOL subscribers each day consists of unsolicited commercial e-mails. [128] Some recipients of commercial e-mail messages also find them an unwanted expense because some internet service providers charge more as consumers receive additional messages. [129]

---

[122] Jill Smolowe, *Read This ! ! ! ! ! ! ! !* Time, Nov. 26, 1990 at 62.

[123] Jill Smolowe, *Read This ! ! ! ! ! ! ! !* Time, Nov. 26, 1990 at 62.

[124] Jill Smolowe, *Read This ! ! ! ! ! ! ! !* Time, Nov. 26, 1990 at 62.

[125] Evan Hendricks, *Capital Insights*, Privacy Times, Dec. 15, 1997, at 1.

[126] Hearings before the H. Com. on Commerce, Subcomm. on Telecommunication, Trade, & Consumer Protection, *Protecting Consumers Against Cramming and Spamming* (Sept. 28, 1998) (Testimony of Randall Boe, Associate General Counsel, American On-Line), available at <http://com-notes.house.gov/cchear> (last checked Oct. 16, 1998).

[127] FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 51 (June 12, 1997) available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Jill A. Lesser, Deputy Director, Law and Public Policy, America OnLine, Inc.). *See also id.*, at 75 (remarks of Colleen M. Kehoe, Graduate Student, Graphics, Visualization and Usability Center, Georgia Institute of Technology) (74% of respondents to survey disagreed strongly that they liked receiving mass e-mailings); Center for Democracy and Technology, Preliminary Comments to the Federal Trade Commission on Unsolicited Commercial E-mail (June 2, 1997), available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/votele.htm> (last checked Aug. 21, 1998) (In response to question, "what do you think of unsolicited commercial e-mail?" 47 said it "is an overall good"; 2196 described it as "a problem;" and 214 called it "overblown as an issue.").

[128] FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 48 (June 12, 1997) available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Jill A. Lesser, Deputy Director, Law and Public Policy, America OnLine, Inc.). *See also id.*, at 64 (remarks of Shabbir J. Safdar, Founder, Voters Telecommunications Watch) (nonrepresentative survey of internet users found that for about a third, spam made up about a quarter of e-mail).

[129] *See* Hearings before the H. Com. on Commerce, Subcomm. on Telecommunication, Trade, & Consumer

Business may also benefit from satisfaction of privacy interests. Thus, a number of commentators and even industry representatives have opined that the internet will not realize its potential as a sales medium unless consumers are assured that their transactions will be private.[130] Polls have reported that privacy is the top reason some consumers have declined to use the internet.[131]

Protection, *Protecting Consumers Against Cramming and Spamming* (Sept. 28, 1998) (Testimony of Paula Selis, Senior Counsel, Consumer Protection Division, Washington State Attorney General's Office), available at <http://com-notes.house.gov/cchear> (last checked Oct. 16, 1998); Voters Telecommunications Watch, *Final Comments to the FTC on Unsolicited Commercial Email*, available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/ftcfilin.htm> (last checked Aug. 21, 1998) (over 2,700 people answered net survey; 2228 stated that unsolicited commercial e-mail cost them long distance or other telephone toll charges; 481 reported that their internet service provider charges them for connect time while they are downloading or reading mail; 76 claimed that their internet service provider charged them by the byte to download mail; and 726 stated that they incurred other costs).

[130] *See, e.g.*, Federal Trade Commission, *Privacy OnLine: A Report to Congress* 43 (1998) ("If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential."); Evan Hendricks, *E-Commerce & Privacy*, Privacy Times, May 29, 1998, at 10 (remarks of Madeline Mooney, vice-president of Lycos Inc., an internet company) (testifying before Congress on the slow progress of electronic commerce: "Privacy concerns are at the heart of this, The majority of Web users today will not provide personal registration information and many say they do not trust sites that collect personal information."); Amy Harmon, *F.T.C. to Call for Laws to Protect Children on Line*, NY Times, June 4, 1998 (quoting Rep. Edward J. Markey as saying "If privacy protections are not built into Internet commerce, then a vast majority of Americans will never trust the Internet."); Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C.L. Rev. 847, 851 (1998) ("if consumers do not trust companies to protect their privacy, the companies will not generate the volume of transactions essential for consumer electronic commerce to be profitable."); John V. Swinson, *Confidentiality on the Superhighway*, Am. Lawyer, Dec., 1995, at 23. *But see* Peter P. Swire & Robert E. Litan, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 88 (1998)) ("Polling data and personal intuition support the argument that people will engage in more electronic commerce if they believe their privacy will be protected. Any such increases may be offset by the decreases in commerce that can occur because of interference with the free market.").

[131] Statement of the FTC on Consumer Privacy on the World Wide Web Before the Subcom. on Telecommunications, Trade and Consumer Protection of the H. Com. on Commerce, July 21, 1998 available at <http://www.ftc.gov/os/9807/privac98.htm> (last checked July 30, 1998) ("A substantial number of online consumers would rather forego information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are."); Evan Hendricks, *Internet Users Want New Privacy Laws, Survey Finds*, Privacy Times, Jan. 2, 1997, at 4, 5 (Poll finds that 66% decline to register with web sites because web site didn't provide clear statement on how information was to be used); Family PC Parents on the Internet Survey available at <wysiwyg://2/http://www.zdnet.com/familypc/content/kidsafety/results/html> (last checked July 30, 1998) ("When asked what the [sic] found most troubling about the Internet for themselves, parents cited abuse of personal information as their chief concern." 88% described that as a concern); Letter of Jerry Berman and Deidre Mulligan, Executive Director and Staff Counsel of the Center for Democracy and Technology to the Federal Trade Commission (June 4, 1997), available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/demotech.htm> (last checked Aug. 21, 1998) (CDT survey showed "A majority of respondents avoid registering at Web sites and giving out personal information for fear of the privacy implications . . . concern about the collection of personal information and the potential harm arising from its misuse were prevalent . . . ."); Comments of trust Concerning Consumer On-Line Privacy submitted to FTC, available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/etrust.htm> (last checked Aug. 21, 1998) (in

B. How much do people say privacy matters to them?

Over the last decade, numerous polls--many of them conducted by Equifax and Alan F. Westin--have fleshed out what consumers say about privacy. A brief summary: on some privacy issues, consumers are united, often taking pro-privacy positions, but sometimes concluding that other values are more important than privacy. On other issues, consumers are not unanimous, but large percentages of them take pro-privacy positions.

1. Issues on Which Consumers Tend to Agree

According to a 1996 survey commissioned by Equifax, 89% of the public is concerned about threats to their personal privacy.[132] Other polls have also found many consumers concerned about the state of their privacy.[133] An increasing number of consumers agrees that consumers have "lost all control over how personal information about them is circulated and used by companies."[134] Nearly four out of every five respondents regards privacy as a fundamental right, worthy of addition to the list in the Declaration of Independence of "life,

---

consumer survey 41% of respondents report leaving Websites when asked to provide registration information on the internet); Evan Hendricks, *House Hearing Covers Self-Regulation, Encryption,* Privacy Times, Apr. 3, 1998 at 2, 3.

[132] Alan F. Westin, *"Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues* in NTIA, *Privacy and Self-Regulation in the Information Age,* available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>. That number has increased slowly, but fairly steadily. For example, in 1994, 84% stated that they were concerned, *Equifax-Harris Mid-Decade Consumer Privacy Survey* 17 (1995); in 1990, 79% were concerned while in 1983 77% were. *1990 Equifax Report supra* note ___ at 2. The 1995 figure was 82%. *Equifax-Harris Mid-Decade Consumer Privacy Survey* 17 (1995). Similarly, one 1998 survey found that 87% of computer users were concerned, Alan F. Westin & Danielle Maurici, *E-Commerce & Privacy* 7 (1998), while another found 88% of consumers concerned. *1998 Privacy Concerns and Consumer Choice Survey,* available on internet at <http://www.privacyexchange.org/iss/surveys/1298execsum.html> (lat checked Dec. 17, 1998).

[133] The Cambridge Reports surveys, conducted in 1988 and 1989, found that more than two-thirds of the respondents called personal privacy "very important" and nearly a quarter called it "somewhat important. More than two-thirds of those queried were either "very concerned" or "somewhat concerned" about invasion of their personal privacy. *See* James E. Katz & Annette R. Tassone, *Public Opinion Trends: Privacy and Information Technology,* 54 Public Opinion Q. 125, 135, 139-40 (1990). A poll by Money magazine found that 74% of the public are somewhat or very concerned about threats to their privacy while 65% are more worried about their privacy than they were five years ago. Ann Reilly Dowd, *Money Poll: You're Deeply Worried About Your Privacy,* Money Mag., Aug. 1, 1997.

[134] Alan F. Westin, *"Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues* in NTIA, *Privacy and Self-Regulation in the Information Age,* available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F> (71% in 1990, to 80% in 1995, to 83% in 1996).

liberty and the pursuit of happiness." [135] One poll found that 98% of consumers believe their privacy is substantially threatened by marketers and advertisers. [136]

On some specific issues consumers are also in accord. For example, 97% of parents with children who use the internet believe web sites should not sell or rent personal information pertaining to children. [137] Nearly three-quarters find it objectionable for a Web site to request a child's name and address even if used solely for internal purposes. [138] A 1991 survey found that more than half the respondents believe it is important for consumers to be able to opt out of the sale of personal information while a third view it as somewhat important. [139] And consumers dislike telphone solicitations: 47% say they are always an intrusion while another 32% find them mostly an intrusion. [140]

While people acknowledge the value of privacy, most value some other things even more. Thus, more than three out of four Americans say they would be very or somewhat upset if they could not obtain credit based on their record of paying bills. [141] Similarly, 96% agree that "when people want to borrow money, the company giving them credit should be able to check on their credit records;" [142] three-quarters feel that businesses should be able to inquire into the

---

[135] 1990 Equifax Report *supra* note ___ at 7.

[136] Survey conducted by Yankelovich Partners, Inc, and reported on at 1993 Direct Marketing Association annual conference, as described in Mary J. Culnan, *Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing*, 9 J. Direct Marketing 10, 11 (1995).

[137] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 6 (1998).

[138] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 6 (1998). Another survey, albeit one that used a sample which was not representative of the public at large, found 93% of the respondents believed the collection of personal information from children to be very serious. *See* AT&T Labs-Research Technical Report TR 99.4.3, BEYOND CONCERN: UNDERSTANDING NET USERS' ATTITUDES ABOUT ONLINE PRIVACY (1999), available at **Error! Reference source not found.** (last checked April 19, 1999).

[139] *Harris-Equifax Consumer Privacy Survey 1991* at 19.

[140] *Privacy Concerns and Consumer Choice Survey*, available on internet at <http://www.privacyexchange.org/iss/surveys/1298execsum.html> (last checked Dec. 17, 1998).

[141] *1990 Equifax Report supra* note ___ at 26.

[142] *Id.* at 44. When asked if they agree that "when people apply for a credit card, the company issuing the credit card should be able to check on their credit and credit card records," 94% said yes. *Id.*

checking performance of those who pay by check; and substantial majorities find it acceptable for companies to check the public record information of consumers applying for auto insurance or jobs.[143]

2. Issues on which Consumers Are Not Unanimous.

Several polls have made it clear that some people do have more of a taste for privacy than others.[144] For example, the 1990 Equifax Report compared certain demographic characteristics with the answers given by respondents to 46 questions. Equifax found that liberals were more privacy-oriented than moderates and conservatives on 23 of the questions; Jews were more privacy-oriented than Protestants and Catholics on 32 of the questions; and those who had read and heard more about consumer privacy issues in the previous year were also more privacy-oriented on 18 questions.[145] The desire for privacy also varied by age [146] and experience with computers.[147] Another survey found that women tend to be more concerned about threats to their privacy than men; [148] that pattern also shows up in connection with privacy on the internet.[149] Notwithstanding Judge Posner's view, the most likely explanation for these different perspectives is that the various groups have different tastes for privacy, rather than that some of these groups have more discreditable information they wish to conceal than others. These broad disagreements in preferences for privacy suggest that any rule designed to accommodate the preferences of different consumers on some issues will need to be flexible.

---

[143] *Harris-Equifax Consumer Privacy Survey 1992* at 5.

[144] *1990 Equifax Report, supra*, note ___.

[145] *1990 Equifax Report, supra*, note ___ at xxv.

[146] *Id.*

[147] *Id.* at xxv-xxvi.

[148] Ann Reilly Dowd, *Money Poll: You're Deeply Worried About Your Privacy*, Money Mag., Aug. 1, 1997 (80% of women concerned about threats to their privacy, while only 68% of men are).

[149] FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 11 (June 11, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Humphrey Taylor, Chair & CEO, Louis Harris & Assoc., Inc).

Many consumers are troubled by the trade in personal information, though some are less concerned and others are not bothered by it at all. Thus, the 1990 Equifax survey showed that while 39% viewed the sharing of information by companies in the same industry as a major problem, 43% called it a minor problem, and 16% said it was not a problem at all. [150] Similarly, though 57% feel that consumers being asked to provide excessively personal information is a major problem, 33% describe it as only a minor problem, and 10% do not perceive a problem at all. [151] A 1996 survey found that half the public is not concerned or only slightly concerned about having their names on mailing lists, while the other half is somewhat concerned or greatly concerned. [152]

Differences of opinion also show up when consumers are asked about solicitations. For example, a 1996 survey found that half of all consumers would prefer not to get any mailings at all, while the other half likes to get mailings on products and services of interest to them. [153] In 1996, 37% of respondents to an Equifax poll said that they regard mail offers as a nuisance, while 43% reported that though they rarely use mail offers they do not see them as a problem, and 12% regard mail offers as a useful opportunity. [154] That survey also found that 55% of the public feel the combination of first, compiling profiles of individual consumers' purchasing

---

[150] *1990 Equifax Report*, *supra*, note ___ at 18.

[151] *Id.*

[152] Beth Negus, *You're Not Welcome; Direct Survey has Alarming Findings About 'Junk' Views and Data Protection*, Direct, June 15, 1996, at 1, 60 (27% were not at all concerned, 23% were slightly concerned, 24% were somewhat concerned, and 25% were greatly concerned).

[153] Beth Negus, *You're Not Welcome; Direct Survey has Alarming Findings About 'Junk' Views and Data Protection*, Direct, June 15, 1996, at 1, 61. *See also id.* at 64 (of the 62% of consumers who said they favor restrictions on data-use, more than three-quarters would still favor such laws even if it meant they would not receive catalogs or mail about things that interest them); *1990 Equifax Report supra* note ___ at 28 (when consumers were asked how they would feel if they could not receive at home mail offers or catalogs geared to their interests, 14% replied that they would be very upset, 25% somewhat upset, 23% would not be very upset, and 38% would not be upset at all).

[154] 1996 Equifax/Harris Consumer Privacy Survey, available at <http://www.equifax.som/consumer/parchive/svry96/docs/summary.html> (last checked July 28, 1998). In 1991, 46% saw mail offers as a nuisance; 38% rarely used them but did not see a problem; and 6% regarded mail offers as useful. *Harris-Equifax Consumer Privacy Survey 1991* at 16-17.

patterns and second, using the profiles to mail offers to consumers is somewhat acceptable; another 11% believe it to be very acceptable; while a third view it as either not very acceptable, or not at all acceptable.[155] Similarly, in 1990 only 23% said they would be very or somewhat upset if they could not receive at their homes, by mail or telephone, new offers of credit, while 21% said they would not be very upset, and 56% said they would not be upset at all.[156]

Though nearly all consumers who receive unsolicited commercial e-mail dislike it, they differ in the intensity of their reactions. One survey found that 42% felt that unsolicited e-mails are "getting to be a real pain and [they] want to stop getting these messages," while 55%--less critical--viewed the e-mails as a little bothersome. Three percent liked receiving the messages.[157] A 1996 survey found 43% of internet users disagreed strongly that on-line providers should be able to track their internet use in order to send them targeted marketing offers; 28% disagreed somewhat; while a quarter agreed somewhat and 4% agreed strongly.[158]

A bare majority complains that existing laws and practices do not adequately protect their privacy.[159] Other polls also demonstrate a split in views.[160]

---

[155] *1996 Equifax/Harris Consumer Privacy Survey* at 84.

[156] *1990 Equifax Report supra,* note ___, at 30.

[157] FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 10 (June 11, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Humphrey Taylor, Chair & CEO, Louis Harris & Assoc., Inc.). *See also* Louis Harris & Associates & Alan F. Westin, *Commerce, Communication, and Privacy Online* 23 (1997); Voters Telecommunications Watch, *Final Comments to the FTC on Unsolicited Commercial Email,* available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/ftcfilin.htm> (last checked Aug. 21, 1998) (unscientific survey; when asked, "What do you think of unsolicited commercial e-mail?" 47 replied that it is an overall good, 2196 called it a problem, and 214 described it as overblown as an issue.); AT&T Labs-Research Technical Report TR 99.4.3, BEYOND CONCERN: UNDERSTANDING NET USERS' ATTITUDES ABOUT ONLINE PRIVACY (1999), available at **Error! Reference source not found.** (last checked April 19, 1999) (52% of unrepresentative sample found unsolicited commercial e-mail very serious).

[158] *1996 Equifax/Harris Consumer Privacy Survey* at 71.

[159] Alan F. Westin, *"Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues* in NTIA, *Privacy and Self-Regulation in the Information Age,* available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F> (54% in 1995). *See also* Beth Negus, *You're Not Welcome; Direct Survey has Alarming Findings About 'Junk' Views and Data Protection,* Direct, June 15, 1996, at 1, 64 (poll found 62% of consumers favor data use restriction laws); Heather Green, Catherine Yang, & Paul C. Judge, *A Little Privacy, Please,* Business Week, Mar. 16, 1998 (50% of computer users said that government should pass laws "now" on whether personal data can be collected and used on the internet).

This variation in views is also shared by executives in privacy-intensive industries, people who can be expected to be more knowledgeable about the extent to which consumer information is available than ordinary consumers. The 1990 Equifax Report indicates that these executives are terribly conflicted about whether the privacy of personal information in computers is adequately safeguarded. Depending on the specific industry, the range of executives who thought it was adequately safeguarded varied from 39% to 57% while the proportion of those who thought it was not ranged from 40% to 57%.[161]

Some of the reported survey results may be affected by the manner in which the question is posed. Even taking that into account, however, it is quite clear from the survey results that many consumers say they are troubled by the availability of information about them, and that many either claim they are not troubled or are not troubled very much. Some also appreciate the major consequence of the trade in consumer information--namely that they receive solicitations at home. It thus seems fair to say that the surveys indicate that consumers are divided.

The survey results have led Alan F. Westin to divide consumers into three groups. [162]

---

[160] For example, the eighth annual survey of the Georgia Institute of Technology's Graphic, Visualization & Usability Center found that 63% of the respondents objected to internet website content providers selling personal information about consumers who visit their sites. Evan Hendricks, *Internet Users Want New Privacy Laws, Survey Finds*, Privacy Times, Jan. 2, 1997, at 4. Similarly, a Business Week/Harris poll found that 39% of respondents who don't use the internet would be more likely to start using it if they had more control over businesses sending marketing messages they didn't want, while 56% said it would not make a difference. Of consumers who had bought things online, 65% said they were very concerned or somewhat concerned that the company they had bought from would use their personal information to send them unwanted information, while 35% said they were not very concerned or not at all concerned. Consumers who had not bought online demonstrated greater concern about the receipt of unwanted information. Thus, 86% were very or somewhat concerned about the possibility of receiving unwanted information from a company they might buy from while only 14% stated that they were not very concerned or not at all concerned. Keith H. Hammonds, *OnLine Insecurity*, Business Week, Mar. 16, 1998. Another poll--of a group which is not statistically representative—found that the respondents "reactions to scenarios involving online data collection were extremely varied. . . . it seems unlikely that a one-size-fits-all approach to online privacy is likely to succeed." AT&T Labs-Research Technical Report TR 99.4.3, BEYOND CONCERN: UNDERSTANDING NET USERS' ATTITUDES ABOUT ONLINE PRIVACY (1999), available at **Error! Reference source not found.** (last checked April 19, 1999).

[161] *1990 Equifax Report*, *supra*, note ___ at 85.

[162] Alan F. Westin, *"Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues* in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>.

Westin describes about 25% of the public as "Privacy Fundamentalists" who tend to reject the view that organizations are entitled to obtain personal information. Privacy Fundamentalists favor strong laws to protect privacy. Westin identifies as "Privacy Unconcerned" people who have little problem supplying personal information to organizations. This group, which Westin believes makes up about 20% of consumers, sees little need for privacy legislation. Finally, the remaining 55% of the public fall into the category of "Privacy Pragmatists." According to Westin, Privacy Pragmatists hold different views on different information activities, depending on such things as whether they trust the particular industry, the value to themselves and society of the particular program calling for the information, whether the information is relevant, and whether fair information practices are being observed. Westin believes that Privacy Pragmatists tend to favor voluntary solutions over legislation, but will support legislation if voluntary approaches fail.

This split shows up in other ways as well. For example, in 1990 Equifax attempted to pose in two different ways questions designed to elicit reactions to the sale of mailing lists. When the questions were posed in one way, 69% described as a "bad thing" that businesses were able to buy mailing-list information about them; [163] of these, 40% described themselves as very concerned about it while another 46% were somewhat concerned. On the other hand, 28% called sales of mailing list information a good thing. [164] When the question was posed another way, a

---

[163] 1990 Equifax Survey at 69. Another poll found 67% concerned about the sale of personalized marketing lists and 69% concerned about internet companies soliciting information about their family's buying habits. Ann Reilly Dowd, *Money Poll: You're Deeply Worried About Your Privacy*, Money Mag., Aug. 1, 1997. Still another found that 68% of consumers regard the collection and distribution of data to marketing companies as a serious invasion of privacy. Survey conducted by Yankelovich Partners, Inc, and reported on at 1993 Direct Marketing Association annual conference, as described in Mary J. Culnan, *Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing*, 9 J. Direct Marketing 10, 11 (1995).

[164] *See 1990 Equifax Report, supra* note ___, at 69. Consumers were told:

> Businesses marketing goods and services directly to consumers are now able to buy from mailing list-making companies information about your consumer characteristics--such as your income level, residential area, and credit card use--and use such information to offer goods and services to you. Do you feel this is a good or bad thing?

better than two-to-one majority found the sale of mailing lists acceptable. [165] It may be that one group consistently view the sale of information about individuals as unfortunate, regardless of how the question is phrased, another group sees it as desirable no matter how the question is put, and a third group is swayed by the wording of the question.

The 1990 Equifax surveyors also asked consumers about pre-screening in two different ways.[166] When the question was put one way, about three-quarters of consumers found pre-screening unacceptable, while another quarter called it acceptable. [167] When they were asked about pre-screening in different words, however, respondents found it acceptable by a better than two-to-one margin.[168] Again, it appears that a hard-core of consumers views pre-screening as

---

Consumers who replied that it is a bad thing were then asked: "How concerned are you about this--are you very concerned, somewhat concerned, not very concerned, or not at all concerned?

Similarly, an American Express telephone survey found that 80 percent of all Americans think that companies should not give out personal information to other companies. Mary Gardiner Jones, *Privacy: A Significant Marketing Issue for the 1990s,* 10 J. Public Pol. & Mktg. 133 (1991).

[165] *See 1990 Equifax Report, supra,* note __ at 71-72. Consumers were told:

> Increasingly, companies are marketing goods and services directly to people by mail. Some reasons for this trend are that many people have less time to shop or they prefer to make shopping decisions at home. Also, companies are trying to reduce their costs of advertising and selling in stores, and they find direct marketing can reduce their expenses and their product prices.
>
> Companies try to learn which individuals and households would be the most likely buyers of their products or service. They buy names and addresses of people in certain age groups, estimated income groups, and residential areas with certain shopping patterns so they can mail information to the people they think will be most interested in what they are selling. Do you find this practice acceptable or unacceptable?

[166] For discussion of pre-screening, see *supra* note ___ and accompanying text.

[167] *See 1990 Equifax Report, supra,* note ___ at 70. Consumers were asked:

> Some companies want to identify consumers with a certain income and a good credit history, to send them an offer for a premium credit card or a product. They ask credit reporting bureaus to screen their computerized files for those who meet the requirements and then supply just the consumer's name and address. However, they do not get the consumer's advance permission. Do you feel this practice is acceptable or is not acceptable?

Just 23% of the respondents answered that the practice was acceptable while 76% found it unacceptable.

[168] *See 1990 Equifax Report, supra,* note ___ at 74-75. Consumers were asked:

> Credit card issuers also market directly to consumers. To make sure they send information only to people who qualify, they ask credit bureaus to tell them which individuals meet their credit standards before they send a credit offer. Is this practice acceptable or unacceptable to you?

When put this way 66% found the practice acceptable and 32% called it unacceptable.

acceptable, another group finds it unacceptable, and a third group's views are affected by the manner in which they are asked. [169]

3. Resolving the split based on information practices.

Westin concluded that the Equifax surveys consistently showed that consumer concern with particular information-gathering practices could be converted to strong majority approval when the information-gatherers employed such fair information practices as notifying consumers what information was being collected, how it was being used, and affording consumers options as to whether the information would be supplied to others. [170] Other surveys also suggest consumers favor disclosure by companies. Thus, a 1991 survey conducted by Time Magazine and the Cable News Network found that 93% of the respondents agreed that companies should be required by law to ask permission from individuals before selling information about them. [171] Similarly, a Money Magazine poll found that 88% of the public favors a privacy bill of rights

---

[169] When Equifax asked about pre-screening again in 1996, in connection with insuance, just over half the public found it "very" or "somewhat" acceptable while another quarter found it "not at all acceptable." *1996 Equifax/Harris Consumer Privacy Survey* at 11.

[170] Alan F. Westin, *"Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues* in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>. Other such fair information practices include limiting the uses of the information to the broad area of consumer activity the individual is knowingly involved in; allowing consumers opportunities to examine and correct the information; and adopting rules to keep information confidential and secure. For examples of the findings supporting Westin's conclusion, *see 1990 Equifax Report, supra*, note ___ at 73, which asked consumers who found the sale of mailing lists unacceptable whether the sale could be made acceptable if people who did not want to receive these offers by mail could have their names excluded. Of those asked, 88% said that would make the practice acceptable, while only 10% said it would still be unacceptable. The same surveyers asked consumers who found pre-screening unacceptable whether it would be acceptable if people who did not want to be offered credit cards by mail could ask not to have their names and addresses used for this kind of screening. Of the respondents, 89% would then see it as acceptable while 9% continued to view it as unacceptable. *1990 Equifax Report, supra*, note ___ at 76. The 1996 Equifax/Harris Privacy Survey found that about nine out of ten consumers found it acceptable for companies to use credit report information to decide which consumers to send pre-approved offers of insurance provided that the consumers had the chance to opt-out of the mailing lists. By contrast, only about half found the practice acceptable if consumers could not opt out. 1996 Equifax/Harris Consumer Privacy Survey, available at <http://www.equifax.som/consumer/parchive/svry96/docs/summary.html> (last checked July 28, 1998).

[171] Evan Hendricks, *Latest Poll Shows Public Concern Over Privacy Continues to Surge*, Privacy Times, Nov. 19, 1991, at 7. Another poll showed a lower percentage, though still a majority of 60%, of consumers object to the sale of mailing lists without permission. Survey conducted by Yankelovich Partners, Inc, and reported on at 1993 Direct Marketing Association annual conference, as described in Mary J. Culnan, *Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing,* 9 J. Direct Marketing 10, 11 (1995).

"that would require companies to tell consumers and employees exactly what kind of personal information they collect and how they use it." [172]

C. How do consumers act to protect their privacy?

Perhaps the most common way in which consumers protect their privacy is to have an unlisted telephone number. Because consumers pay for unpublished listings, the listings also say something about how much consumers value their privacy: in theory, consumers with unlisted numbers value their privacy at least as much as it costs to conceal their phone number. The numbers of consumers willing to pay for an unpublished number varies from state to state. In California, 55% of residential telephone numbers are not listed, while in New York State 24% maintain unpublished numbers. [173]

Other evidence too, indicates that some consumers value privacy highly. Some claim to have acted on their privacy preferences. The 1990 Equifax Report found that 30% of Americans say they decided against applying for something, like a job, credit, or insurance, because they did not want to reveal certain information about themselves. [174] Though it is impossible to know precisely what information was concealed, the authors of the 1990 Equifax Report commented that the increase in the percentage of Americans who have chosen not to apply for some benefit rather than to provide the information sought "may be a strong indicator, in practical terms, of the unease felt by the American public concerning how personal information is used by large organizations." [175]

---

[172] Ann Reilly Dowd, *Money Poll: You're Deeply Worried About Your Privacy*, Money Mag., Aug. 1, 1997.

[173] Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>.

[174] *See 1990 Equifax Report, supra*, note ___ at 13.

[175] *Id. See also* Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing, and Consumer Privacy: Ethical Issues*, 12 J. Public Pol. & Marketing 106, 115 (1993) (quoting voter whose personal information was used because of voting as saying "I have voted in every election since I was 18, and I think [this] was the last

Similarly, the Federal Trade Comm ission has observed that "a substantial number of online consumers would rather forgo information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are."[176] The 1995 Equifax survey found that 59% of the public has refused to give information to a business because they thought the information was either not needed or was too personal.[177] Significantly, pollsters found in 1990 that those who can be expected to know best about the uses of information--executives in privacy -intensive industries such as lending and direct marketing--were even more likely to withhold requested information than the rest of us.[178]

Consumers have acted in other ways to protect their privacy. Some have tried to prevent even the creation of databases. For example, Lotus Development Corporation and Equifax engaged in a joint venture to develop a database on a compact disc that would contain the names, addresses, personal buying habits, and income levels of about 120 million Americans.[179] The data base, dubbed "Marketplace: Households," would have been available at a price small businesses and nonprofit organizations could afford, and could have been extremely useful to many of them. As one commentator explained, "the owner of a trendy new restaurant could get a list of young, affluent people living near his establishment. A local political organization could target older, married homeowners in a given neighborhood."[180] But the companies abandoned Marketplace: Households after receiving some 30,000 calls, e-mails, and letters of complaint

---

election I'll ever vote in.").

[176] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 3 (1998). *See also 1998 Privacy Concerns and Consumer Choice Survey*, available on internet at <http://www.privacyexchange.org/iss/surveys/1298execsum.html> (last checked Dec. 17, 1998) (78% of consumers "say they have refused to give information to a business or company because they thought it was not really needed or was too personal.").

[177] *Equifax-Harris Mid-Decade Consumer Privacy Survey* 3 (1995).

[178] *1990 Equifax Report, supra*, note ___ at 15.

[179] *See* Daniel Mendel -Black & Evelyn Richards, *Peering into Private Lives*, Washington Post, Jan. 20, 1991, at H1, H6; Jacob Sullum, *For Sale*, Reason, Apr. 1992, at 29.

[180] Jacob Sullum, *For Sale*, Reason, Apr. 1992, at 29.

from people who were concerned about having their names included. [181] It is impossible to know how many people heard about Marketplace: Households and did not care enough to complain (or did not care at all, or even looked forward to the product). But 30,000 people valued their privacy enough to invest in a complaint. Consumer complaints have also caused other businesses to abandon plans which some feel would have infringed upon consumer privacy. [182]

IV. The Conflicts Between What Consumers Say and What They Do.

A. Few Consumers Opt Out.

Given the survey and other evidence discussed above, we might expect to see that consumers generally have not taken steps to prevent the use of their credit reports in rulings on credit applications but that many consumers have acted to prevent the sale of their personal information for marketing purposes. We might also expect that others permit the use of their

---

[181] See Daniel Mendel-Black & Evelyn Richards, *Peering into Private Lives*, Washington Post, Jan. 20, 1991, at H1. Mendel-Black and Richards elaborated on Marketplace: Households:

> Information for the disc was gleaned from 40 different sources, including the U.S. Census, Internal Revenue service, Postal Service and surveys taken at 8,500 shopping centers and retailers nationwide. As one of the country's largest credit bureaus, Equifax has also drawn on its own records, which contain specific information about a person's marital status, sex, age range and likely income level. . . . The most sensitive information--estimated income and lifestyle--is blended with that of nearby households to build a general profile for each neighborhood. And a user would not be able to seek out a specific person. In other words, a user could not look up John Q. Smith on Aurora Drive, but Smith's name and address would pop up as part of a larger group of people fitting a certain profile. The companies say this and other measures will help protect privacy.

Id. at H6. Consumer Reports, working with a demonstration disc, reported that the program allowed users to limit searches to particular streets or even certain buildings, and that depending on the attributes searched, lists could have fewer than ten households on them. *See What Price Privacy?* Consumer Reports 356, 360 (May 1991).

In the end, consumers may have scored an incomplete victory. Other CD-ROM products are available, and a competitor of Equifax, Experian (formerly TRW), has announced plans to produce a product similar to Marketplace: Households. Mary J. Culnan, *Self-Regulation on the Electronic Frontier: Implications for Public Policy*, in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>.

[182] *See, e.g.*,, Evan Hendricks, *Capital Insights*, Privacy Times, June 28, 1996, at 1 (Lexis-Nexis dropped plan to make consumer Social Security numbers available to subscribers after complaints); Evan Hendricks, *Capital Insights*, Privacy Times, May 2, 1996, at 1 (After receiving complaints, Database America and Yahoo! deleted 90 million unlisted numbers from what was to be compilation of 175 million names and addresses); *Pac Bell Backs-off Selling Lists*, Alameda Times Star, Apr. 16, 1986 (company reversed decision to sell customer names and addresses after receiving more than 75,000 customer protests); Seth Schiesel, *America Online Backs Off Plan to Give Out Phone Numbers*, N.Y. Times, July 25, 1997 (company abandoned plan to provide lists of phone numbers to telemarketers and others within 24 hours after plan became widely known and consumers complained).

personal information for marketing, in accordance with their preferences. This is what Coase's famous theorem appears to predict, at least at first glance. [183] Coase maintained that when people could bargain freely without transaction costs--an important limitation which will be discussed below--their bargaining would produce an efficient allocation of resources regardless of which party initially possessed the relevant property right. [184]

The Coase theorem suggests that people who value their privacy more than the information is worth to firms would pay businesses not to keep the data. [185] Conversely, if the firms value the data more than people value their privacy, people would not wish to pay the businesses enough to make the businesses willing to forgo use of the data, and the businesses would continue using the information.

Now assume that the law forbids the operation of databases on people, unless the affected individuals consent to collection and distribution of the information. Again, if privacy is worth more to people than the information is worth to firms, the firms will not be able to pay people enough to make them give up their right to privacy and no databases will be in operation. Alternatively, if the firms value the information more than people value privacy, the firms will purchase from people the right to run the databases. [186]

---

[183] *See* Ronald Coase, *The Problem of Social Cost*, 3 J. L. & Econ. 1 (1960).

[184] In Richard A. Epstein's words:

> The law may create any distribution of entitlements that it chooses, be it wise or foolish. In the next instant, all the relevant parties can enter into as many transactions as they please and thereby correct any ostensible misallocations created by the legal order. No matter how Byzantine the legal system's initial rules, private parties and government actors collectively can cut the Gordian knot and in a twinkling move resources to their highest -valued use.

Richard A. Epstein, *Holdouts, Externalities, and the Single Owner: One More Salute to Ronald Coase*, 36 J. L. & Econ. 553, 555 (1993).

[185] *See* Richard A. Epstein, *Holdouts, Externalities, and the Single Owner: One More Salute to Ronald Coase*, 36 J. L. & Econ. 553, 558 (1993) ("In principle, if the transactions costs between the two parties were low enough (zero is always low enough), then B [individuals] would be able to pay A [the firms] some sum of money to alter those activities that would leave both parties better off than they would be in the absence of that bargain.").

[186] *See also* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Georgetown L. J. 2381, 2413 (1996) (suggesting that merchants could purchase rights from consumers

In either case--whether the law gives firms the right to operate databases or people the right to keep businesses from operating databases--the Coase theorem predicts the same outcome. If firms value the information more, the databases will come into existence; if people value privacy more, there will be no databases. [187]

In fact, comparatively few consumers seem to have taken steps in a systematic fashion to bar marketers from using their personal data. True, some consumers have acted to curtail the number of solicitations they receive. A number have even paid fees to services which purport to reduce or eliminate commercial solicitations. [188] Some consumers have asked enterprises to add their names to "opt-out" lists, that is, lists of consumers who do not wish to receive solicitations. [189] The Direct Mailing Association ("DMA"), a trade association of firms involved with direct mail, maintains a list of 3.3 million consumers who have indicated that they do not wish to receive direct mail. [190]

Other prominent examples of consumers opting out exist: in 1990, the company then known as New York Telephone allowed consumers to have their names deleted from the list that the telephone company planned to sell to direct marketers. Of the 6.3 million customers to

---

by price differentiation; that is, by charging consumers who withheld permission to use their personal information a higher price than consumers who granted permission).

[187] Coase's theorem has elicited some critical academic discussion, some of which is referred to in Christine Jolls, Cass R. Sunstein, & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 Stan. L. Rev. 1471, 1483 (1998) ("The Coase theorem . . . can lead to inaccurate predictions.").

[188] Perhaps the most prominent of these services is Public Citizen, Inc. A website operated by Consumer Net lists several of the companies which provide these services. The website is at <http://consumer.net/optout/consumerfee.asp> (last checked on July 8, 1998). *See also* Gini Graham Scott, *Mind Your Own Business* 321 (1995). Florida has a system in which its residents can pay ten dollars to have telemarketers told not to call them. Annual renewals cost five dollars. Fla. Stat. § 501.059. Two years after the system's inauguration, 25,000 Floridians had paid the ten dollars. William M. Bulkeley, *Congress's 'Cure' for Junk Calls Runs into Skepticism at the FCC*, Wall St. J., May 19, 1992 at B6.

[189] Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Public Pol. & Marketing 149, 157 (1991); Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 333 (1996) (noting that American Express and Citibank notify cardholders each year that they may opt out).

[190] Letter from Michael D. McNeely, Assistant Director, FTC Bureau of Competition, to Robert L. Sherman, dated Sept. 9, 1997, available at http://www.ftc.gov//os/9710/dma.htm. DMA also maintains a second list of consumers who object to telemarketing calls.

whom the offer was made, 800,000 opted out.[191]

But while the total number of consumers who have opted out seems large, the percentage of consumers who have opted out is not large at all. Commentators estimate that the proportion of consumers who take advantage of opt outs is twenty percent or even less.[192] That permits the inference that few consumers genuinely care about solicitations; the assumption is that if consumers cared, they would act on their preferences.

B. Are the Surveys Inaccurate?

How can this be reconciled with the survey evidence which suggests that so many consumers find the trade in information objectionable? One possibility is that the surveys do not accurately report consumer preferences. Survey evidence should always be viewed with skepticism, and there are a number of reasons why that is particularly so with privacy surveys.

First, all of this discussion assumes that consumers view the competing costs and benefits of solicitations and privacy the same way at all times regardless of what they are being solicited to buy. In fact, that may not be so. A personal example makes the point. In 1995, my wife died. My daughters were then three and five years old. To save time, I began purchasing my daughters' clothing from catalog companies. Initially the catalogs I selected clothes from were

---

[191] Anne Wells Branscomb, *Who Owns Information?* 15 (1994). Ultimately, New York Telephone abandoned its plan to sell the list because of consumer opposition. U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 7, n. 26 (1995).

[192] Priscilla M. Regan, *Legislating Privacy* 233 (1995). In the fall of 1997, Maryland adopted a system in which drivers could block access to information pertaining to them. By March 1, 1998, 646,000, or about 17 percent of the State's 3.8 million drivers, had opted out. Rajiv Chandrasekaran, *Doors Fling Open to Public Records*, Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy9.htm> (last checked June 15, 1998). *See also* Laurie Peterson, *The Great Privacy Debate*, ADWEEK Western Advertising News, Sept. 23, 1991, at p. S24 ("Studies show that when given the choice, fewer than 10% of consumers will ask to receive no more catalogs."); Karlene Lukovitz, *Cashing in on Renting Your List*, Folio, Oct. 1985, at 106 ("Publishers interviewed by FOLIO uniformly reported that very few readers take advantage of the option to not have their names rented; CBS, for instance, gets such requests from under 2 percent of subscribers . . . ."); FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 40 (June 12, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Jill A. Lesser, Deputy Director, Law and Public Policy, America OnLine, Inc.) (about half a million members of AOL have opted out during AOL's existence).

addressed to my wife, but after I made my purchases, the successor catalogs came addressed to me. Over time, I began to receive catalogs from companies I had not bought from, presumably because they had acquired my name from the companies whose clothes I had purchased. I was grateful for these additional catalogs because they increased the choices available to my daughters and me.

Eventually, however, I began to receive catalogs from companies that sold women's clothing, including at least one which sold rather intimate apparel. Once again, I surmise that these companies had purchased my name from companies which sold me children's clothing, I suppose on the assumption that people who buy clothes for children also buy garments for women.[193] These catalogs I was not so pleased to receive. Putting aside the fact that lingerie hardly suits me, I did not need to be reminded about my wife's death by receiving catalogs which should have come to her. But the point is, if I had been asked my views about the selling of my name and about privacy, how should I answer? I wanted my name to be sold to some companies but not others. I welcomed some solicitations but was saddened by others. My answers might have varied at different times--depending on which catalog I had received last, or upon whether I had recently ordered clothing for my daughters--and also would have been different if I could have focused on some catalogs and not others. But the surveys are not that narrowly tailored.

My specific situation is unusual, fortunately.[194] But what may not be unusual is that

---

[193] My guess is that it is more than just an assumption. That is, I suspect that the companies which sell women's clothing have found that they will sell more if they send their catalogs to people who buy children's clothing from catalogs.

[194] Others have discussed the pain direct marketers can unwittingly cause. *See, e.g.*, R.J. Ignelzi, *Mail and Telejunk*, San Diego Union-tribune, July 4, 1995 at E1 (woman who had miscarriage received for years solicitations which assumed birth of baby, including birthday cards); Erik Larson, *The Naked Consumer* 11, 83-86, 204-05 (1992) (predicting that solicitations would be sent to families that had lost children given child-mortality rates; author told one magazine that imaginary person in his household was expectant mother; imaginary person subsequently received dozens of mailings, including more than a hundred offers; advice columnist describes "sadness, shattered feelings, family rifts, grief, doubt, and devastation" caused by direct mail ads which included handwritten notes from direct mailer suggesting recipient try anti-aging creams, diet pills and the like; notes confused recipient into thinking someone they knew had sent them the ad); Privacy Rights Clearinghouse, S*econd Annual Report of the Privacy Rights Clearinghouse* 24 (1995) (junk mail still sent to person who died six years after

consumer preferences may shift depending on when the questions are posed, what recent experiences the consumer has had, and whether the consumer has most recently received a solicitation which the consumer was interested in receiving or objected to. Surveys offer support for the notion that consumers do not view all solicitations the same way. The 1996 Equifax/Harris Privacy Survey found that if consumers were offered the choice of having their names removed from all mailing lists, some mailing lists or no mailing lists, three out of four would have their names deleted from some. [195] Only 15% would have their names removed from all lists; 12% would not have their names deleted from any. [196] Strikingly, among those who say they have experienced invasions of privacy, or think of mail offers as invasions of privacy or a nuisance, about two-thirds would still keep their names on some direct mail lists. [197] Consumers also have different reactions to different commercial e-mail offers. [198] The data available probably leave the picture of consumer preferences incomplete, but given the limitations of surveying--the need to keep consumers answering questions without compensation for a fairly long time--perhaps it is simply impossible to obtain more useful information than we have. Whether this particular problem would under-report or over-report concern for privacy is

---

death; woman who miscarried receives baby-related catalogs two years later).

[195] 1996 Equifax/Harris Consumer Privacy Survey, available at <http://www.equifax.som/consumer/parchive/svry96/docs/summary.html> (last checked July 28, 1998). *Cf. Panel One: Information Issues: Intellectual Property, Privacy, Integrity, Interoperability, and the Economics of Information*, 48 Fed. Com. L. J. 5, 41 (1995) (remarks of Ellen Kirsh, Vice-President, General Counsel, and Secretary of America OnLine, Inc .) ("I think that if people are given the choice, there is some information that they'd like to get. If you don't want Publisher's Clearinghouse, maybe there are some things that you would like people to send to you, if there is some reasonable way to do that, that could turn out to be a good thing for everyone.").

[196] Similarly, the 1991 Harris-Equifax Consumer Privacy Survey found that 64% would choose to have their names removed from some lists, 22% from all lists, and 13% from no lists. *Id.* at 18-19.

[197] 1996 Equifax/Harris Consumer Privacy Survey, available at <http://www.equifax.som/consumer/parchive/svry96/docs/summary.html> (last checked July 28, 1998).

[198] *See* Louis Harris & Associates & Alan F. Westin, *Commerce, Communication, and Privacy Online* 23 (1997) ("If a procedure <u>were</u> available to block their e-mail addresses from product and service offers, 37% of Interent and online service users who send or receive e-mail would want their addresses blocked from <u>all</u> offers. A large group (50%) would want their address blocked from <u>some</u> offers, and the smallest group (12%) would <u>not</u> want their addresses blocked at all.") (emphasis in original).

impossible to determine.

A second problem with relying on survey evidence suggests, however, that surveys may systematically under-report consumer concern for privacy. The consumers who care most about privacy are not likely to answer survey questions precisely because of that concern. [199]

A third problem implies that the surve ys may over-report privacy concerns. It has been suggested that survey respondents who realize that they are being queried about privacy may reply with answers they think the pollsters want to hear, even if the respondents did not previously hold those views.[200]

C. Why Consumers Might Not Opt Out.

But other, more persuasive, explanations for the disparity between how the surveys suggest consumers should behave and how consumers actually do behave are possible. Opt-out lists may not accurately reflect consumer interest in opting out, for several reasons.

1. Consumers Don't Know About Opt Outs or How Their Personal Information is Used.

First, consumers may not take advantage of opt-out lists because they may not know about them. Thus, critics say that even more consumers would have opted out of the New York Telephone list if the telephone company had done a better job of informing consumers that they could do so.[201] Roughly fifty percent of the nation's consumers are said to be unaware of the DMA list--or, in fact, any program for deleting their names from marketing lists. [202] Similarly, the

---

[199] Priscilla M. Regan, *Legislating Privacy* 49 (1995).

[200] Priscilla M. Regan, *Legislating Privacy* 49 (1995).

[201] Dottie Enrico, *Dollars and Dialers; Phone Company's Plan to Sell Names Stirs Controversy*, Newsday, June 11, 1990, at 3.

[202] 1996 Equifax/Harris Consumer Privacy Survey, available at <http://www.equifax.som/consumer/parchive/svry96/docs/summary.html> (last checked July 28, 1998) ("The percentage of people who report being aware of any procedures that allow one to remove one's name from direct mail lists for catalogs, products, and services has remained constant from 1991 to the present at 44%.); *Harris-Equifax Consumer Privacy Survey 1991* at 18; Mary J. Culnan, *"How Did they Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use*, MIS Quarterly, Sep. 1993, at 341, 357 (78% of participants unaware of procedures to allow mailing list removal). *See also* Louis Harris & Associates & Alan F. Westin, *Commerce, Communication, and Privacy* Online 23 (1997) (57% of computer users aware of

1996 Equifax/Harris poll found that only 29% of those who find mail solicitations an invasion of privacy know about procedures to have their names removed from mailing lists. [203]

Indeed, few consumers even understand how much of their personal information is for sale. While consumers may know generally that there is a trade in personal data and that information about that trade is kept from them--a poll found that 90 percent of Americans think that companies don't disclose enough about their list usage [204]--many consumers remain largely unaware of how businesses use information about them. [205] Even fairly sophisticated consumers

---

procedures that allow them to remove names from direct mail lists for catalogs, products and services, and 25% of online service and internet users who send or receive e-mail know of procedures for removing their e-mail addresses from companies that send e-mail offers). *Cf.* Gerald Tolchin, *Personal Privacy and Access to Information on a College Campus: A Preliminary Report,* 29 Psychology-A Journal of Human Behavior 12, 14 (1992) (about half students surveyed were aware of or seemed to understand certain of their privacy rights under the Family Education Rights and Privacy Act of 1974).

[203] 1996 Equifax/Harris Consumer Privacy Survey, available at <http://www.equifax.som/consumer/parchive/svry96/docs/summary.html> (last checked July 28, 1998). One study of the 1991 Equifax-Harris Consumer Privacy Survey data found that those who were not aware of name removal procedures are less concerned about privacy measured by whether consumers feel they have lost control but more concerned about privacy measured by their answers to a question about privacy as an overall concern. They also felt that having the opportunity to opt out is less important than did those who were aware of procedures for opting out. Mary J. Culnan, *Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing,* 9 J. Direct Marketing 10, 14-15 (1995).

[204] Mary Gardiner Jones, *Privacy: A Significant Marketing Issue for the 1990s,* 10 J. Public Pol. & Mktg. 133 (1991).

[205] *See* Smith, *supra* note ___ at 4 (study finds "consumers tend to be quite uninformed regarding the actual [privacy] policies and practices of industries with which they deal regularly."); Privacy Rights Clearinghouse, First Annual Report (1994) available on the web at <http://www.privacyrights.org/ar/annrept.html> (last checked Oct. 6, 1998) ("Most [consumers] are unaware of the ways in which personal information is . . . used and distributed . . . ."); Alan F. Westin, *"Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues* in NTIA, *Privacy and Self-Regulation in the Information Age,* available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F> (1997 survey concerning online privacy "found that 71% of respondents online were not aware of their services' information policies . . . and that most visitors to web sites were not aware of the policies those sites followed in collecting visitors' personal information."); Ticked Off At Amex, USA Today, May 26, 1992 at 10A (consumer assumed that personal data provided to credit card companies and other lenders protected by a business ethics code); Simson L. Garfinkel, *How Computers Help Target Buyers, Businesses Screen and Identify Potential Customers with Information from Credit-Bureau Databases,* Christian Science Monitor, July 25, 1990 at 13 (quoting Bonnie Guiton, Special Adviser for Consumer Affairs to President Bush as saying "A major concern of mine is that consumers are uninformed. . . .In most cases, they don't even know that (information on them) is being collected."); Robert O'Harrow, Jr. *Are Data Firms Getting Too Personal?* Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy/8.htm> (last checked June 15, 1998) (quoting Leslie L. Byrne, former director of the U. S. Office of Consumer Affairs as saying "most people don't have a clue what's being gathered about them."); Frank V. Cespedes & H. Jeff Smith, *Database Marketing: New Rules for Policy and Practice,* Sloan Management Rev., summer 1993 at 7, 8 ("Our interviews with consumers . . .suggest that they are still largely unaware of how information about them is gathered and used . . . ."). *Cf.* Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace,* 1996 U. Chi. L. Forum 77, 107 ("Consumers

may not be fully informed about the use of their personal information: how many readers of this article were surprised by the information described as being available in its first pages? [206]

One study found that a reason consumers may not know firms' information policies is that executives intentionally hide them. [207] The study reported that when consumers learn of the information practices, "they often become angry and call for legal intervention." [208]

Paul M. Schwartz, discussing medical data, has argued that when consumers believe that their records are protected from disclosure and that businesses know that in fact the records are not subject to such protections, a monopoly equilibrium exists. [209] Empirical studies seem to confirm the insight that sellers have disproportionate market power when consumers possess imperfect information. [210] In such circumstances, sellers can be expected not to compete on the

---

generally were not aware that calls made to 800 and 900 number information services, especially to '976' or other sexually oriented services, generated transaction records."). Peter Swire has pointed out that consumer ignorance of company use of their personal information may have significant costs: "Because the company internalizes the gains from using the information, but can externalize a significant share of the losses, it will have a systematic incentive to over-use private information. In terms of the contract approach, companies will have an incentive to use private information even where the customers would not have freely bargained for such use. Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information,* in NTIA, *Privacy and Self-Regulation in the Information Age,* available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>.

[206] This lack of awareness of consumers by consumers creates other problems as well. For example, because consumers do not know what information is collected about them, they cannot correct errors in that information. *See* Reidenberg, *Setting Standards, supra,* note ___ at 534 .

[207] *See* Smith, *supra* note ___ at 4. *See also* Robert O'Harrow, Jr. *Are Data Firms Getting Too Personal?* Wash. Post, March 8, 1998 at A1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/privacy/8.htm> (last checked June 15, 1998) ("That obfuscation is sometimes intentional, according to Maryalice Hurst, former chairman of the Direct Marketing Association's ethics committee. Some companies 'go behind the customers' back to acquire what they know the customer wouldn't give them,' Hurst said.")

[208] Smith, *supra* note ___ at 4.

[209] *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 Tex. L. Rev. 1, 49 (1997).

[210] For example, a number of studies have found that increased comparison shopping by consumers leads to lower market prices. *See, e.g.,* D. Grant Devine & Bruce W. Marion, *The Influence of Consumer Price Information on Consumers and Grocery Retailers: Some Preliminary Findings of a Field Experiment,* 16 J. Consumer Affairs 224 (1982); Kenneth McNeil et al., *Market Discrimination Against the Poor and the Impact of Consumer Disclosure Laws: The Used Car Industry,* 13 Law & Soc'y Rev. 695, 708-09 (1979); J. Edward Russo et al., *An Effective Display of Unit Price Information,* J. Mktg., Apr. 1975, at 11. *See also* E. Thomas Sullivan & Brian A. Marks, *The FTC's Deceptive Advertising Policy: A Legal and Economic Analysis,* 64 Or. L. Rev. 593, 620 (1986) ("The courts, the Commission, and legal commentators have recognized that the lack of product information leads to market imperfections, abuse and related consumer welfare."); Steve Salop, *Information and Market Structure: Information*

basis of how much security they provide for information, but instead to exploit consumer ignorance.[211] To put it more bluntly, how can consumers who do not know the consequences of providing personal information decide whether they want to provide the information? [212]

2. The Difficulty of Opting-Out.

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. An amusing story in The New York Times makes the point:

> Mary R. Sive has had it with junk mail. Wherever possible, she telephones companies with 800 numbers and asks that they remove her name from their database. "Do not send a catalogue," she says, and the request has succeeded to some extent, but her latest call had an unusual result. She received a catalogue but her name had indeed been eliminated. The mailing label was now addressed to "Do not send a catalogue." [213]

But consumers seeking to remove their names from lists face other, more troublesome obstacles. Even if consumers can obtain the information needed to opt-out, the cost of communicating and negotiating with all the relevant information-gatherers, in terms of time and money, may be substantial. [214] Anne Wells Branscomb described her experiences: "attempting

---

and Monopolistic Competition, 66 Am. Econ. Rev. 240 (1976) ("if information is costly, each small firm obtains market power, and the equilibrium (if one exists) is characterized by prices above competitive levels. . . "); William N. Eskridge, *One Hundred Years of Ineptitude: The Need for Mortgage Rules Consonant with the Economic and Psychological Dynamics of the Home Sale and Loan Transaction*, 70 Va. L. Rev. 1083, 1112, n.96 (1984); Phillip Nelson, *Information and Consumer Behavior*, 78 J. Pol. Econ. 311 (1970); Charles Stuart, *Consumer Protection in Markets with Informationally Weak Buyers*, 12 Bell J. Econ. 562 (1981). *But see* Leon Courville & Warren H. Hausman, *Warranty Scope and Reliability Under Imperfect Information and Alternative Market Structures*,52 J. Bus. 361, 373 (1979) ("inaccurate information does not imply poor market results" based on an economic model that makes the questionable assumption that consumers maximize perceived expected utility).

[211] *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 Tex. L. Rev. 1, 49 (1997).

[212] *Cf.* Fair Packaging and Labeling Act, Pub. L. No. 89-755, 80 Stat. 1296 (1966) (codified at 15 U.S.C. §§ 1451-61) ("informed consumers are essential to the fair and efficient functioning of a free market economy."); FTC, Statement of Basis and Purposes, Labeling and Advertising of Home Insulation, 44 Fed. Reg. 50218, 50223 (1979) (" An essential element of effective competition is the availability of information that consumers need to evaluate competing products and to make the best possible choices."); Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 765 (1976) ("the free flow of commercial information is indispensable" to free enterprise economy).

[213] Enid Nemy & Ron Alexander, *Metropolitan Diary*, NY Times, May 4, 1998 at B2, col. 3.

[214] *See* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of*

to get out of the clutches of the database managers is almost a full-time job. I can vouch for this, because I have spent the last five years trying to withstand the assault of direct mail marketers on the post office box I rented to relieve the overstuffed mailbox at my home address."[215] Other stories are similar: one consumer still receives junk mail after having written over 2,000 letters seeking deletion from mailing lists. [216] Not even telemarketing executives--presumably more knowledgeable than the rest of us about avoiding solicitations--can escape: the president of one telemarketing company tells telemarketers who call him at home that he died. [217] As Joel Reidenberg has written, "this obscured transparency raises transaction costs and allocates them

---

Personal Information, in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F> ("It is a daunting prospect for an individual consumer to imagine bargaining with a distant Internet marketing company or a huge telephone company about a desired privacy regime. To be successful, bargaining would likely require a considerable degree of expertise in privacy issues, as well as a substantial commitment of time and effort. The cost of this elaborate bargaining process is likely to exceed the incremental benefit in privacy to that citizen."); Meheroo Jussawalla & Chee-Wah Cheah, *The Calculus of International Communications: A Study in the Political Economy of Transborder Data Flows* 80 (1987) ("Bargaining over contract terms is not usually possible. First of all, a data subject acting on his own accord would normally be incapable of preparing a valid agreement without incurring substantial costs. Second, there are no economies to be gained from bargaining unless the frequency of information disclosures and potential costs of privacy invasions are sufficiently high to warrant employment of legal expertise. Third, privacy invasion is sufficiently unlikely in any discreet transaction so that the expected costs of privacy invasion are marginal compared to the costs of bargaining."); Sandra Byrd Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?* 48 Fed. Communications L. J. 163, 165 ("Contractual solutions burden the data subject with the task of tracking personal information already collected and then trying to stop its dissemination, rather than requiring the broker who wishes to sell that information to first obtain consent for its release.").

[215] Anne Wells Branscomb, *Who Owns Information?* 11 (1994). *See also* Evan Hendricks, *Junk Mail Leading Cause of Complaints to Calif. Hotline*, Privacy Times, May 19, 1995, at 1, 3:

> The [Privacy Rights Clearinghouse] has attempted to obtain the consumer profile of one of its staff members from several of the compilers, to no avail. They do not appear to have developed the infrastructure to respond to such requests. Yet, a basic privacy protection principle is that individuals should "have the right to ask whether personal data about him/her appear on a direct marketer's file and to receive a summary of the information within a reasonable time after the request is made."

[216] Privacy Rights Clearinghouse, S*econd Annual Report of the Privacy Rights Clearinghouse* 25 (1995). *See also* G. Bruce Knecht, *Privacy: Junk-Mail Hater Seeks Profits From Sale of His Name*, Wall St. J., Oct. 13, 1995, at B1 (Consumer who for years has requested companies to delete his name from their mailing lists still receives one to seven solicitation letters each day).

[217] Caroline E. Mayer, *Telemarketers Answering Their Calling*, Wash. Post, August 31, 1997 at H1, available at <http://www.washingtonpost.com/wp-srv/frompost/march98/sidebars/phone/10.htm> (last checked June 15, 1998).

to citizens."[218]

Special problems in opting out arise in the e-mail context. Many e-mail direct marketers view requests from consumers asking to be removed from lists as confirmation that the e-mail has been received, and continue to send e-mail to the offended consumer, or even flame the customer.[219] Indeed, this practice is so widespread that some advise consumers unhappy with the promotional e-mails they receive not to seek name-removal. [220] Consumers who learn that lesson in the e-mail context may carry it over to other contexts as well, and so refrain from asking to be deleted from direct mail lists.

Of course the DMA has its opt-out lists. But the DMA lists are of limited utility. Many direct marketers eschew the DMA mail list, perhaps because DMA charges for it. [221] Only a

---

[218] Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector,* 80 Iowa L.Rev. 497, 533 (1995).

[219] Ann Reilly Dowd, *Protect Your Privacy,* Money Mag., Aug. 1, 1997:

> Spammers often punish those who try to opt out of getting unsolicited e-mail by "flaming" them--sending them nasty messages online, sometimes in overwhelming numbers. Just ask David Aronson, a Dulles, Va. software engineer and outspoken spam critic. On top of the 20-odd spams he received at work and home on an average day, Aronson showed MONEY a stream of filthy utterly unprintable flames from someone who described himself as a "gay atheist commie spammer." Warns Aronson: Never, ever reply directly to spammers. It tells them your e-mail address is valid. They will sell it, and you'll get more spam.

See also FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 11 (June 12, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Jason Catlett, Chief Executive Officer, Junkbusters Corp.) (Some spammers "actually maintain their own pseudo-remove addresses but simply use the results as an additional source of addresses to spam."); Letter from John R. Levine to FTC (Apr. 27, 1998) available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/jrlevine.htm> (last checked Aug. 21, 1998) ("sending remove responses as often as not results in the recipient receiving more rather than less junk mail, since spammers usually add all addresses on all mail they receive to their mailing lists for future ads. (Many of my acquaintances have verified this by sending a remove request from a freshly created e-mail address that has never been used before, only to start receiving junk e-mail at that address.)."); Hearings before the H. Com. on Commerce, Subcomm. on Telecommunication, Trade, & Consumer Protection, *Protecting Consumers Against Cramming and Spamming* (Sept. 28, 1998) (Testimony of Paula Selis, Senior Counsel, Consumer Protection Division, Washington State Attorney General's Office), available at <http://com-notes.house.gov/cchear> (last checked Oct. 16, 1998) ("Prior state experience demonstrates that most senders of [unsolicited commercial e-mail] don't stop sending e-mail when asked."). The problem is exacerbated by the fact that there is no way to designate e-mail addresses as unpublished, as there is for telephone numbers. *See* John V. Swinson, *Confidentiality on the Superhighway,* Am. Lawyer, Dec., 1995, at 23.

[220] Amy Harmon, *How to, Well, Eat Less Spam,* N.Y. Times, May 7, 1988 at G8.

[221] Allison Fahey, *DMA Speaks to Consumers,* Advertising Age, Apr. 9, 1990, at 63.

fraction of all firms engaged in direct marketing are members of DMA, and some of these non-members are the companies most likely to misbehave, [222] though DMA members are said to account for a major percentage of the direct mail solicitations in this country. [223] Registering with DMA will not help with the mailing lists of political organizations, non-profits, or local retailers.[224]

The DMA members themselves are hardly role-models: reportedly, only about half the DMA members use the DMA mail preference service to screen their mailings. [225] Even when companies buy the DMA list, consumers may not be completely satisfied: lists are sold so frequently that sometimes names are sold faster than they can be deleted. [226] Hence, one privacy group claims that "consumers who attempt to make use of the Direct Marketing Association's Mail Preference Service routinely report that they continue to receive junk mail and that the service is not effective."[227]

---

[222] *Phone Soliciting--For Whom the Bell Tolls*, Consumer Reports 356, 360 (May 1991) ("[S]hady operators are usually not [Direct Marketing A]ssociation members."); Ann Reilly Dowd, *Protect Your Privacy,* Money Mag., Aug. 1, 1997 ("many of the worst offenders are, naturally, not DMA members."); Comments of the Electronic Privacy Information Center Concerning Children's Privacy to the FTC available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments3/epic3.html> (last checked Aug. 21, 1998) (noting that self-proclaimed largest bulk advertising e-mailer in country is not a member of DMA).

[223] Letter from Michael D. McNeely, Assistant Director, FTC Bureau of Competition, to Robert L. Sherman, dated Sept. 9, 1997, available at http://www.ftc.gov//os/9710/dma.htm.

[224] Nora Carrera, *One Man's Junk is Another's Mail*, Rocky Mountain News, Sept. 25, 1995, at 38A.

[225] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 333 (1996) (citing Mary J. Culnan, *Consumer Attitudes Toward Secondary Information Use, Privacy and Name Removal: Implications for Direct Marketing*, paper presented at Symposium on Consumer Privacy, Chicago/Mid-West Direct Marketing Days, Jan. 20, 1993).

[226] Susan Headden, *The Junk Mail Deluge*, U.S. News & World Rep., Dec. 8, 1997. *See also* R. J. Ignelzi, *Mail and Telejunk*, San Diego Union-Tribune, July 4, 1995 at E1 ("It takes between two and six months to have your name and address removed from mailers' lists.").

[227] Comments of the Electronic Privacy Information Center Concerning Children's Privacy to the FTC available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments3/epic3.html> (last checked Aug. 21, 1998). *See also* Mark Lewyn, *You Can Run, But It's Tough to Hide from Marketers*, Bus. Week, Sept. 5, 1994 (consumers who use DMA list say their names come off some, but not all lists); Comments of Beth Givens, Project Director, Privacy Rights Clearinghouse to FTC (Apr. 14, 1997) available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/sess2com.htm> (last checked Aug. 21, 1998) ("Does the [DMA list] work? From the standpoint of callers to the PRC's hotline who have used the [DMA list], the answer is "no." Consumers see little to no reduction in volume of unsolicited mail after registering with the [DMA]. The only category of mail for which the [DMA] has any noticeable effect is catalog mail.")

Moreover, companies using the DMA opt-out list remain free to maintain and develop profiles on consumers; they are only called upon to refrain from soliciting consumers on the list.[228] One frequent commentator on privacy has opined that the DMA list is "meaningless" and "just a public relations effort."[229]

Still another significant problem with the DMA lists is that placing your name on them is an all-or-nothing proposition for companies that use them: consumers do not have the option of telling DMA which solicitations they would like to receive and which they disdain. [230] I have chosen not to join the DMA's Mail Preference Service for just that reason, and I am not alone; as discussed above, many consumers would prefer to receive only some of the solicitations currently furnished them. [231]

Consumers who are knowledgeable enough about privacy to be aware of the DMA lists may also understand their limitations. Surely some, mindful of those limitations, have chosen not to write to DMA. Too, some consumers may not take advantage of the DMA lists because of doubts about how effective a trade organization is at protecting consumers: the 1994 Equifax Survey found that about three-quarters of consumers were skeptical that companies offering products or services through the mail or via the telephone would use personal or confidential information in a proper manner--the lowest proportion of any industry asked about. [232] Another

---

[228] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 333 (1996).

[229] Mark Lewyn, *You Can Run, But It's Tough to Hide from Marketers,* Bus. Week, Sept. 5, 1994 (quoting Evan Hendricks, editor of Privacy Times).

[230] *See* DMA, *Fair Information Practices Manual* § 2 at 25 (1994). *See also* Judith Waldrop, *The Business of Privacy,* American Demographics, Oct. 1994 at 46 (quoting Keith Wardell of Buyer's Choice Media).

[231] *See supra* notes ___ and accompanying text. *See also* Judith Waldrop, *The Business of Privacy,* American Demographics, Oct. 1994 at 46 (quoting Keith Wardell of Buyer's Choice Media as saying "what most consumers really mean when they opt out is that there are certain things they want and certain things they don't want. The customer wants to have more control than an absolute on-and-off switch.").

[232] Equifax-Harris Consumer Privacy Survey 6-7 (1994) (for companies that offer products or services through the mail, 47% were not at all confident and 31% were not very confident; the comparable figures for those making telephone offers were 54% and 29%; only 5% and 4% were very confident in the use by these companies of information). *See also* 1990 Equifax Survey, *supra*, note ___ at 20-21 (64% of the public had a low degree of trust in the way companies that solicit people by direct mail or telephone collect and use personal information; consumers

survey found many consumers do not trust companies marketing products on the internet either.[233] Indeed, there are reasons to harbor doubts about some marketers, as the preceding paragraphs make clear.

a. Why is it Difficult to Opt-Out?

Why is it so difficult for consumers to opt-out? The answer to that question might turn on the motivation of businesses in offering an opt-out system at all. Some companies might do so because they are genuinely concerned about the privacy of their customers.

Other companies might wish to offer for sale a list which excludes customers who opt out. Some argue that such a list might command a premium per name, because it should contain a higher proportion of consumers who are interested in receiving solicitations, and thus more likely to buy in response to solicitations.[234] My own experiences suggest at least some direct marketers are not very concerned with pruning their lists, however. Though my wife has been dead since 1995, we still regularly receive junk mail addressed to her.[235] Telemarketers still call to speak to her from time to time. Companies which genuinely want to eliminate poor sales

---

were more willing to trust every other industry asked about, with the percentage of consumers who had a low degree of trust ranging from 18%--for hospitals--to 39%--for credit bureaus). Another survey, conducted by Direct, a trade publication for direct marketers, found that 56% of consumers think direct marketers are generally less honest than other businesses. Beth Negus, *You're Not Welcome; Direct Survey has Alarming Findings About 'Junk' Views and Data Protection*, Direct, June 15, 1996 at 1, 64.

[233] FTC, Public Workshop on Consumer Information Privacy, Session Three: Children's OnLine Privacy, at 157-58 (June 12, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Alan Westin, Editor and Publisher, Privacy and American Business, and Professor, Columbia University) (48% of consumers and 31% of parents of children using the net trusted companies collecting personal information on the net to use information in a proper manner, compared to 77 to 80% confidence in employers, hospitals and banks; 75% of computer users and 82% of net parents said they would not be confident that companies would use personal information collected from children who visited their web sites consistently with the policies they posted at their web sites).

[234] *See* G. Bruce Knecht, *Privacy: Junk-Mail Hater Seeks Profits From Sale of His Name*, Wall St. J., Oct. 13, 1995, at B1 quoting Eli Noam, professor of finance and economics at Columbia Business School as saying "It is true that the costs go up when people can call to remove their names, but the lists that result would be much more selective. . . . Rather than bombarding people with piles of uninvited mail, companies would focus on the people they really want to reach.").

[235] This is not unusual. *See* Privacy Rights Clearinghouse, S*econd Annual Report of the Privacy Rights Clearinghouse* 24 (1995) (person who died six years ago still receives direct mail ads); Widows and Widowers Newsletter, Sept. 25, 1998 (deceased people still receiving mailings).

prospects as a means of making their lists more valuable should probably start with those who have died.[236] Yet at least some do not.

Or perhaps companies which offer their customers an opportunity to opt out are interested in preserving customer good will, possibly for marketing advantages. [237] Consumers who are concerned about privacy might prefer a company which respected their wishes. Even consumers who do not value privacy might favor such a company for respecting consumer concerns.

A handful of companies have in fact chosen to compete on the ba sis of privacy.[238] Gini Graham Scott has written of a mall in West Covina, California, where marketers offered shoppers the opportunity to win money, vacations, and other prizes in return for personal information such as reading habits, purchasing plans, and income level. [239] About 13,000 consumers signed up during the first four months. A number of services on the internet give consumers electronic coupons or discounts in exchange for their information. [240] In the long distance telephone market, one company has advertised that it will not use customer calling

---

[236] My wife's death occasioned an obituary in the New York Times, on August 10, 1995. If they wished to, marketers could keep up with obituaries just as they keep up with birth announcements. For discussion of how marketers learn about and respond to births, see David Zielinski, *Database: The Heart of Relationship Marketing*, 27 Potentials in Marketing 66, 67 (Apr. 1994) (diaper manufacturer knows names of over 75% of expectant mothers in U.S.; information obtained from doctors, hospitals, childbirth trainers). S *ee generally* Erik Larson, *The Naked Consumer* (1992).

[237] *See* Ann Cavoukian & Don Tapscott, *Safeguarding Your Privacy in a Networked World* 179 (1997) ("Treating your customers with respect and recognizing their right to privacy will not only improve customer service but may also create a loyal following, which in turn will boost the bottom line."); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector,* 80 Iowa L.Rev. 497, 535 (1995) ("business is beginning to grasp that better standards for fair information practice can be a competitive advantage and will be necessary for business survival").

[238] At least two businesses have voluntarily decided to use an opt-in system: the Microsoft Network, commonly known as MSN, and USA Today. Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* 69-70, 94-95 (1997).

[239] Gini Graham Scott, *Mind Your Own Business* 322 (1995).

[240] Neil Munro, *Putting a Price on Technology,* 11 Wash. Technology, No. 23, Mar. 6, 1997; Paulette Thomas, '*Clicking' Coupons On-Line has a Cost: Privacy,* Wall St. J., June 18, 1998, at B1(100,000 consumers signed up in first three monthes to receive coupons in return for personal information). *See infra* note ___ and accompanying text.

records to identify and solicit others, while another company apparently does just that. [241]

But these stories are exceptions.[242] For the most part, companies have chosen not to compete on the basis of privacy and not to offer incentives to surrender privacy. [243] Why is that? Perhaps merchants would rather not focus on privacy in advertising for fear that it will obscure more persuasive appeals. Mary Gardiner Jones has suggested that businesses will not compete on privacy because "it falls into the category of 'negative' information about a company." [244] She argues that businesses have little incentive to make investments to protect the security of their information systems and so are unlikely to advertise that their practices are risk-free. [245] In fact, sellers may choose not to advertise product attributes for a variety of reasons.[246]

---

[241] Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>. Similarly, a credit card company now includes in its solicitations a statement that it will not sell customer names to other companies. John N. Frank, *The Brouhaha Over Privacy*, Credit Card Management, May, 1996, at 32, 33. *See also* G. Bruce Knecht, *Privacy: Junk-Mail Hater Seeks Profits From Sale of His Name*, Wall St. J., Oct. 13, 1995, at B1 (American Express, Citicorp, and Dow Jones & Co. reported to allow consumers to opt-out because of desire not to upset their customers). Richard S. Murphy has collected two examples of companies which conspicuously tell consumers that they do not sell their mailing lists. One of these is Radio Shack which posts signs to that effect near its cash registers; the other sells sexual products. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Georgetown L. J. 2381, 2413-14 nn. 165 & 166 (1996).

[242] *Cf.* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1248 (1998) ("For numerous reasons . . . individuals and information collectors do not generally negotiate and conclude express privacy contracts . . . .").

[243] In some market sectors, in which all service in a particular geographical area is provided by a single seller--as is common with utilities and cable TV providers, for example--competition of any sort, including competition on privacy, may not exist, because there are no alternative service providers. *See* U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 20 (1995). That problem may be solvable by regulation, however, just as other problems created by the necessarily-monopolistic nature of some service providers are solved.

[244] Mary Gardiner Jones, *Privacy: A Significant Marketing Issue for the 1990s*, 10 J. Public Pol. & Mktg. 133 (1991); *see also* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L. J. 2381, 2414 (1996) ("Raising the privacy issue may evoke negative reactions in consumers who otherwise would not have thought about the issue."); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1254 (1998) ("Providing a menu of privacy options, with the necessary detail to comprehend them, would draw attention to unsavory privacy practices that the collector may not want to highlight.").

[245] Jones notes too that consumers are not in a position to verify claims that information is in fact secure. In addition, Jones observes, businesses typically do not use a practice mandated by regulation as a promotional tool. Among the example she cites are statutorily-required consumer benefits like unit pricing, full warranties, full disclosures in product descriptions, affirmative disclosures in product descriptions, and ingredient listings.

[246] *See, e.g.*, E. Patrick McGuire, *Industrial Product Warranties: Policies and Practices* 10 (1980) (study

Other, more cynical, explanations exist for companies offering opt outs, and these reasons have little to do with customer satisfaction. Some have suggested that businesses adopt opt-out systems to forestall more draconian governmental regulation. [247] Indeed, the DMA--an organization which has announced that its members must comply with its opt-out system by July 1999--has lobbied extensively against privacy legislation and started its opt-out lists in part to avoid such legislation. [248] Such legislation is a real possibility. In recent decades, a number of governmental entities in the United States, Europe, and Canada have wrestled with informational privacy issues and have produced documents suggesting or mandating, in one form or another, adoption of certain fair information practices. [249] These documents agree that fair information practices include, among other things, that businesses give consumers notice before collecting information from them, and that consumers have options as to how the information collected from them will be used. [250]

Nevertheless, companies may not be eager to offer opt outs because they may rationally

---

of 369 manufacturers found 57% did not advertise warranty terms, for such reasons as terms are too complex, lengthy, and extraneous to seller's main advertising goals); Ian Ayres & F. Clayton Miller, *"I'll Sell It to you at Cost": Legal Methods to Promote Retail Markup Disclosure*, 84 Nw. U. L. Rev. 1047, 1055-56 (1990) (car dealers do not disclose markups even though different dealers use different markups and consumers pay third parties for markup information).

[247] *See* Gary Levin, *DMA to Battle Tougher Privacy Laws,* Advertising Age, Nov. 2, 1992 at 15 (noting that DMA president Jonah Gitlitz urged DMA members to adopt opt-out policy to stave off threat of legislation).

[248] With respect to DMA lobbying, *see* Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues,* 12 J. Pub. Pol. & Mktg. 106, 113 (1993); Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 309 n.5, 332 (1996) (DMA provides "lobbying guidebook to its members that includes sample letters for correspondence with legislators" and "the industry objects to proposals for mandatory opt-out requirements."); Evan Hendricks, *DMA Will Raise $2.6 Million War Chest to Fight U.S. & State Privacy Measures,* Privacy Times, Apr. 22, 1992 at 2. With respect to the DMA's motivation in starting its opt out lists, *see* Alan F. Westin & Michael A. Baker, *Databanks in a Free Society; Computers, Record-Keeping and Privacy* 166 (1972).

[249] *See, e.g.*, United States Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens* (1973); Privacy Protection Study Commission, *Personal Privacy in and Information Society* (1977); Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995); *The European Union Directive on the Protection of Personal Data* (1995); Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

conclude that they incur costs when consumers opt-out--while receiving few offsetting benefits. To the extent that consumers exercise the option of having their names deleted, the company's mailing lists shrink and presumably become less valuable. [251] Moreover, the company incurs transaction costs not only in notifying consumers of the existence of the opt-out option, but also in responding to consumers who opt out.[252]

Companies could respond to these costs by, in essence, charging consumers for opting out. This charge could be imposed in a number of ways, including, for example, offering a discount to consumers who do not opt out.[253] A downside of this approach, however, is that it might generate consumer resentment, conceivably causing some consumers who might otherwise have purchased the company's product to walk away from the transaction altogether. Perhaps the fear of this is why so few sellers offer the differential pricing scheme. Consequently, in the end, sellers who offer opt-out systems appear to absorb the costs of doing so themselves.

Accordingly, companies might decide that, for various reasons, they must offer an opt-out plan, but at the same time not want consumers to take advantage of it. [254] If that were so,

---

[250] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 7, 8 (1998).

[251] Although, as noted above, note ___ and accompanying text, by including only the names of those consumers who wish to receive mailings, and who are thus presumably more open to direct marketing purchases, the companies may make their lists more valuable. Whether the list ultimately increases or decreases in value is a function of whether list purchasers will increase what they pay per name for a "pruned" list enough to compensate for the loss of the names; how many consumers actually opt out; how many do not opt out; and the costs of administering the opt-out program.

[252] *See, e.g.*, FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 223 (June 11, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Martin Nisenholtz, President, New York Times Electronic Media Co., Coalition for Advertising Supported Information and Entertainment) (noting that when consumers ask Times to do something in connection with the Times website privacy policy, Times incurs costs of around $5 per person to manage).

[253] *See* Anthony D'Amato, *Comment: Professor Posner's Lecture on Privacy*, 12 Ga. L. Rev. 497, 501 (1978) (magazine publishers could institute a two -tiered subscription price: those who do not want their names sold would pay more). *See also* Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy*, 12 J. Public Pol. & Marketing 106, 109 (1993) ("One possible solution to this particular dilemma would be to offer consumers a choice of paying interest that reflects the full costs of granting credit or allowing the personal information they provide to be used for unrelated, money-generating purposes to defray some of the costs of granting credit.").

[254] *Cf.* Karl Dentino, *Taking Privacy into our Own Hands; Direct Mail and Telemarketing; Creative*

companies might understandably provide an opt-out mechanism without making it easy for consumers to opt out.[255] To put it another way, companies which offer opt-outs have an incentive to increase transaction costs incurred by opting-out consumers.

This explains why Coase's Theorem has not , by and large, operated to produce a market in privacy and consumer information: as Coase himself recognized, the Coase theorem is a prisoner of its underlying assumption of no transaction costs. That assumption does not apply here.

Avery Katz has identified two types of transaction costs: costs of implementation and costs of strategic behavior.[256] He defines implementation costs as "the real resources used up in bringing contracting parties together, in executing and administering the resulting agreement, in enforcing any bargain reached, and in settling any disputes that arise along the way." [257] In an opt-out context, implementation costs might include the costs incurred when consumers communicate with the marketer that they wish their names excluded from the marketer's list.

Katz describes strategic behavior costs as the "losses suffered because bargainers have the incentive to maximize their individual gains rather than the total surplus from exchange." [258]

Strategies, Direct Marketing Mag., Sept., 1994, at 38:

> Offer opt-out, but carefully . . . . opt-out programs can be a double-edged sword. Ask someone if they want to stop getting phone calls--when 99 out of 100 are not relevant--and what answer do you think you'll get? It's human nature to overlook the offers you do respond to and find of interest. So there's an unconscious classification that happens, and profitable, responsive people might say "no" without really meaning it.
>
> To complicate things further, the people who select the opt-out option might be the most responsive segment of your customer base. A person who goes through the physical act of reading the opt-out offer and responding accordingly is a person who takes the time to read and throughtfully consider direct mail offers.

[255] *Cf.* Douglas Whitford, *The Functions of Disclosure Regulation in Consumer Transactions*, 1973 Wis. L. Rev. 400, 436-37 (discussing possibility that one purpose of consumer regulation is to create illusion that law is pro-consumer without actually helping consumers).

[256] *See* Avery Katz, *The Strategic Structure of Offer and Acceptance: Game Theory and the Law of Contract Formation*, 89 Mich. L. Rev. 215, 225 (1990).

[257] *Id.*

[258] *Id.* at 226.

To the extent that sellers can create these costs, they can reduce the number of consumers who opt out, while preserving their own profits from selling consumer information.

But why wouldn't consumers respond to the increased transactions costs by forgoing the purchase? Some consumers seem to do just that when it comes to the internet. Nevertheless, many consumers buy goods and services through other media which permit the collection of their personal information. Again, some consumers may not know of the uses to which their information is being put. Still, why would knowledgeable consumers make such purchases?

A rational consumer who understands that buying a particular product means surrendering some privacy or invoking an opt-out should still make the purchase if the value to the consumer of having the product exceeds the price plus the lesser of the cost to the consumer of opting out or the value to the consumer of the lost privacy.[259] The idea may be expressed as follows, where V_P is the value of the purchase to the consumer, P is the price, C_{OO} is the cost of opting out, and V_{LP} is the value to the consumer of the lost privacy:

(1) Consumer should buy if $V_P > P +$ (lesser of C_{OO} and V_{LP})

The reason the consumer should focus on the lesser of the cost of opting out and the value to the consumer of the lost privacy is that if the cost of opting out exceeds the value to the consumer of opting out, a rational consumer should not opt out but simply endure the loss in privacy. On the other hand, if the cost of opting out is less than the value of surrendering the lost privacy, a rational consumer should opt out. In either case, the lesser cost is the one that should be relevant.

If businesses inflate the cost to consumers of opting out, some consumers should respond by declining to buy, and so businesses will lose sales. It therefore seems counterintuitive that businesses will inflate the costs to their customers, especially since those costs do not represent

[259] I discuss below some relevant ways in which consumers may not be rational.

revenues received by the businesses themselves, for the most part. But recall that a number of businesses generate more revenue from sales of mailing lists than from the products they offer to consumers. Such businesses have an incentive to inflate the costs to consumers of protecting their privacy until the loss of profit from sales of products to consumers exceeds the loss of profit from the sale of consumer information. Moreover, because many consumers apparently do not know how businesses use their information, the number of consumers who actually decline to buy because of high privacy transaction costs may be low.

This discussion assumes that consumers are rational and knowledgeable about companies' information practices. But what if consumers are not knowledgeable about information practices? Then consumers should buy if the value of the product to them exceeds the price. Or, put another way:

(2) Consumers should buy if $V_P > P$

In this second equation, consumers who care about their privacy end up losing it, but they do not take that into account in deciding whether to make the purchase. Presumably, some nescient consumers will end up purchasing, using the formula in equation (2), who would not have bought if they had knowledgeably used the formula in equation (1). Such purchases actually reduce society's net welfare, but they increase the share of the pie provided to sellers, who realize the profit both on the sale of something to consumers and the sale of consumers' personal information--which may be another reason why sellers do not, with some exceptions, publicize their information practices.

How do companies increase consumers' transaction costs in opting out? A brochure titled "Privacy Notice" which my local cable company included with its bill provides an example.[260] This Privacy Notice discussed, among other things, how cable subscribers could

[260] Under the Cable Communications Policy Act of 1984, as amended by the Cable Television Consumer

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 papers in the mailing. The Privacy Notice arrived with a bill and the monthly listings for Pay-Per-View, both likely to be of greater interest to many consumers than printed inserts enclosed in the envelope. Social scientists have found that many consumers are more likely to focus on "vivid" information--such as the Pay-Per-View Listings, which were written in considerably more exciting prose, with color photographs--than on duller information. [261] Similarly, many consumers focus more on pictures--again, like those in the Pay-Per-View Listings--than on text. [262]

A story makes the point even more clearly: some years ago, federal regulati on required a bank to send its customers a mailing explaining their rights concerning electronic fund transfers. Perhaps mischievously, the bank promised in 100 of the pamphlets that it would send $10 to any customer who sent in his or her name and address on a sheet of paper with the word "regulation." No one responded to the promise.[263]

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

Protection and Competition Act of 1992, 47 U.S.C. §§ 521, cable television companies may not sell their subscriber lists unless they give subscribers the opportunity to opt out. *See generally* Michael I. Meyerson, *The Cable Communications Policy Act of 1984: A Balancing Act on the Coaxial Wires,* 19 Ga. L. Rev. 543, 615-17 (1985).

[261] *See* Richard E. Nisbet & Lee Ross, *Human Inference: Strategies and Shortcomings of Social Judgment* 45 (1980); Margaret G. Wilson et al., *Information Competition and Vividness Effects in On-Line Judgments*, 44 Organizational Behav. & Human Decision Processes 132 (1989); Jonathan Shedler & Melvin Manis, *Can the Availability Heuristic Explain Vividness Effects?* 51 J. Personality & Soc. Psychol. 26 (1986).

[262] *See* Richard E. Nisbet & Lee Ross, *Human Inference: Strategies and Shortcomings of Social Judgment* 51 (1980); Robert E. Gehring et al., *Recognition Memory for Words and Pictures at Short and Long Retention Intervals*, 4 Memory & Cognition 256 (1976); Roger N. Shepard, *Recognition Memory For Words, Sentences, and Pictures*, 6 J. Verbal Learning & Verbal Behav. 156 (1967).

[263] The story is told in Alan Schwartz & Robert E. Scott, *Commercial Transactions: Principles and Policies* 1142 (2d ed. 1991).

While some reports are to the contrary, many studies have now demonstrated the existence of "information overload;" that is, the idea that consumers when overloaded with information either do not make optimal decisions, or that overwhelmed consumers simply overlook relevant information. [264] This is not necessarily irrational behavior: some argue that contracting parties rationally do not read contractual terms because of the cost of reading through the terms and the likelihood that the information provided is not useful. [265] Consequently, some consumers may be deterred from reading the brochure, or at least from finishing it, by its length. An interesting contrast is again provided by the Pay-Per-View listings, which typically provide only a brief paragraph about each movie or event.

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. For example, some

---

[264] *See, e.g.*, Kevin L. Keller & Richard Staelin, *Effects of Quality and Quantity of Information of Decision Effectiveness*, 14 J. Consumer Res. 200, 211 (1987); John C. Bergstrom & John R. Stoll, *An Analysis of Information Overload with Implications for Survey Design Research*, 12 Leisure Sciences 265 (1990); Naresh K. Malhotra, *Information Load and Consumer Decision Making*, 8 J. Consumer Res. 419 (1982). Early studies included Jacob Jacoby, et al., *Brand Choice Behavior as a Function of Information Load: Replication and Extension*, 1 J. Consumer Res. 33 (1974); and Jacob Jacoby et al., *Brand Choice Behavior as a Function of Information Load*, 11 J. Marketing Res. 63 (1974). For criticism of the early Jacoby studies, *see, e.g.*, Naresh K. Malhotra, *Reflections of the Information Overload Paradigm in Consumer Decision Making*, 10 J. Consumer Res. 436 (1984) (suggesting that information overload does occur, but that the early Jacoby studies did not demonstrate it); J. Edward Russo, *More Information is Better: A Reevaluation of Jacoby, Speller & Kohn*, 1 J. Consumer Res. 68 (1974); John D. Summers, *Less Information Better?*, 11 J. Marketing Res. 467 (1974); William L. Wilkie, *Analysis of Effects of Information Load*, 11 J. Marketing Res. 462 (1974). For Jacoby's replies, see Jacob Jacoby, *Constructive Criticism and Programmatic Research: Reply to Russo*, 2 J. Consumer Res. 154 (1975); and Jacob Jacoby, *Information Load and Decision Quality: Some Contested Issues*, 14 J. Marketing Res. 569 (1977). For studies rebutting the information overload effect, *see* Debra L. Scammon, *"Information Load" and Consumers*, 4 J. Consumer Res. 148 (1977); Naresh K. Malhotra et al., *The Information Overload Controversy: An Alternative Viewpoint*, 46 J. Marketing 27 (1982); and Thomas E. Muller, *Buyer Response to Variations in Product Information Load*, 69 J. Applied Psych. 300 (1984). For criticism of these last studies, *see* Jacob Jacoby, *Perspectives on Information Overload*, 10 J. Consumer Res. 432 (1984). For criticism of the Keller & Staelin study cited above, *see* Robert J. Meyer & Eric J. Johnson, *Information Overload and the Nonrobustness of Linear Models: A Comment on Keller & Staelin*, 15 J. Consumer Res. 498 (1989). Keller and Staelin's response appears at *Assessing Biases in Measuring Decision Effectiveness and Information Overload*, 15 J. Consumer Res. 504 (1989). For law review discussions of information overload, *see* Robert E. Scott, *Error and Rationality in Individual Decisionmaking: An Essay on the Relationship between Cognitive Illusions and the Management of Choices*, 59 S. Cal. L. Rev. 329 (1986); David M. Grether et al., *The Irrelevance of Information Overload: An Analysis of Search and Disclosure*, 59 S. Cal. L. Rev. 277 (1986), criticized in Melvin Eisenberg, *Text Anxiety*, 59 S. Cal. L. Rev. 305 (1986).

[265] *See, e.g.*, Avery Katz, *The Strategic Structure of Offer and Acceptance: Game Theory and the Law of Contract Formation*, 89 Mich. L. Rev. 215, 273 (1990).

companies state only that they may make offers they "think would be of interest to you."[266] While some companies may make this limited disclosure in good faith, commentators have suggested that "the vagueness intentionally avoids giving individuals knowledge of actual practices."[267]

A third reason why consumers receiving the Privacy Notice may not read it stems from its prose. Notwithstanding our local Plain Language Law,[268] computer analyses of the text found it extremely difficult, requiring more than a college education for comprehension.[269] For purposes of comparison, the computer found a draft of this article considerably easier going than the Privacy Notice.[270]

Fourth, 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.[271]

My cable company is hardly unique in the presentation of its opt-out policy. Another

---

[266] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 280 (1996).

[267] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 280 (1996).

[268] NY Gen. Obl. L. § 5-702 (written consumer agreements to be "[w]ritten in a clear and coherent manner using words with common and every day meanings. . . ."). Strictly speaking the Plain Language Law does not apply to the Privacy Notice because the statute governs only written agreements, and the Notice is not an agreement. Still, properly construed, the Plain Language Law should have some persuasive effect on virtually all documents for consumers.

[269] The Flesch Reading Ease score was 28; the scale ranges from zero (hardest) to 100 (a fourth grade level). Scores between zero and thirty are considered to require a college education or more. By contrast, the Flesch Reading Ease score for this article is 42.8. The Flesch-Kincaid Grade Level required for comprehension of the Privacy Notice was 15.1, higher than the 12.4 Grade Level of this article.

[270] *See supra* note ___.

[271] *Cf.* Charles D. Raab, Colin J. Bennett, Robert M. Gellman & Nigel Waters, APPLICATION OF A METHODOLOGY DESIGNED TO ASSESS THE ADEQUACY OF THE LEVEL OF PROTECTION OF INDIVIDUALS WITH REGARD TO PROCESSING PERSONAL DATA: TEST OF THE METHOD ON SEVERAL CATEGORIES OF TRANSFER 161 (1998) available at **Error! Reference source not found.** ("Some companies that offer an opt-out require consumers to send a letter separately from an order and to a different address" but noting example of company that offers easy to use opt out).

example: in 1996, Congress amended the Fair Credit Reporting Act to provide that information that would otherwise be covered by the statute could be shared among businesses that were commonly owned "if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons." [272] Notwithstanding the "clearly and conspicuously" requirement, the Office of the Comptroller of the Currency is reported to have found that "few banks highlight this option." [273] Acting Comptroller of the Currency Julie Williams has commented that "Most bank customers can't ever recall seeing something like this."[274] And, she has observed:

> it has been known to happen that the affiliate-sharing "opt-out" disclosure is buried in the middle or near the end of a multi-page account agreement. For existing accounts, some institutions have gotten into the habit of reducing the required "opt out" disclosures to the fine print along with a long list of other required disclosures. Few consumers are likely to have the fortitude to wade through this mass of legal verbiage, and fewer still will take the time to write the required "opt out" letter. I have even heard of people getting two separate notifications covering different types of information, requiring two separate letters to opt out.[275]

---

[272] 15 U.S.C. § 1681a(d)(2)(A)(iii). The sharing of personal information among corporate affiliates could be particularly significant for companies with subsidiaries serving different consumer markets. One writer has raised, for example, the possibility of Citibank declining mortgage applications because of information provided a Travelers' insurance agent, now that the two companies have merged, or a consumer receiving a solicitation from Quick & Reilly, a brokerage house, because the consumer made a large deposit in a Fleet Bank account, given that Fleet owns Quick & Reilly. Leslie Wayne, P*rivacy Matters: When Bigger Banks Aren't Bettter,* NY Times, Oct. 11, 1998, § 4, at 4.

[273] Leslie Wayne, P*rivacy Matters: When Bigger Banks Aren't Bettter,* NY Times, Oct. 11, 1998, § 4, at 4.

[274] Leslie Wayne, P*rivacy Matters: When Bigger Banks Aren't Bettter,* NY Times, Oct. 11, 1998, § 4, at 4.

[275] Remarks by Julie L. Williams, Acting Comptroller of the Currency before the Banking Roundtable Lawyers Council (May 8, 1998), available at <http://www.occ.treas.gov/ftp/release/98%2D50a.txt> (last checked Oct. 13, 1998). *See also* Remarks by Julie L. Williams Before the Consumer Bankers Association (Oct. 26, 1998) available at <http://www.occ.treas.gov/ftp/release/98-109a.txt> (last checked Nov. 11, 1998):

> We can find too many disclosure statements that lack specificity, clarity, and simplicity. They are too often opaque and obscure, rather than 'clear and conspicuous.' They place the burden on customers to provide a long list of information, including, in at least one case, account numbers for each account for which information is not to be shared. Too often we found disclosure information in fine print, buried in a mass of equally tiny type, along with other required terms and disclosures. In short, we continue to find that consumer anxieties--based on the lack of clarity and consistency in banks' disclosure policies and practices--are not entirely unfounded.

Not surprisingly, banks are not the only companies that provide opt-out notices in small print.[276] Similar complaints have been made about online disclosures of privacy policies. [277] And other examples are not hard to find. Thus, in 1995, TRW (now Experian) published a booklet titled "Twelve Common Questions about Consumer Credit and Direct Marketing." It is not until the twelfth--and last--question, beginning on the sixteenth page, that the booklet addresses how to remove names from TRW's marketing list. Earlier questions include such inquiries as "How does a credit bureau help me?" [278]

When a merchant provides some information in exciting language with colorful pictures and allows subscribers to make purchase decisions by telephone, while providing the same subscribers a lengthy, dull statement of their rights written in difficult language, calling upon subscribers who object to communicate their views in a separate writing, I wonder how helpful

---

[276] David J. Klein, Note, *Keeping Business out of the Bedroom: Protecting Personal Privacy Interests from the Retail World*, 15 J. Computer & Info. L. 391, 398 (1997) ("List creators generally place [opt-out provisions] in the fine print with other boilerplate terms of the contracts; thus the clause is not readily apparent to most consumers.") (footnotes omitted); Privacy Rights Clearinghouse, S*econd Annual Report of the Privacy Rights Clearinghouse* 27 (1995) ("Disclosure statements . . . are still nonexistent, vague, and/or minuscule. . . The opt-out box on consumer surveys . . . are located in extremely small print at the end, not the beginning of the form."); Mark Lewyn, *You Can Run, But It's Tough to Hide from Marketers*, Bus. Week, Sept. 5, 1994 ("Consumer advocates complain that [opt-out] provisions don't work because most are written in tiny type."); Erik Larson, *The Naked Consumer* 90 (1992) (describing how company prints opt-out notice in "print exactly the size of the *E Pluribus Unum* on a nickel").

[277] FTC, Public Workshop on Consumer Information Privacy, Session Three: Children's OnLine Privacy, at 218 (June 12, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Mary Ellen Fise, General Counsel, Consumer Federation of America) ("While a few attempts are being made in this area, for the most part, we found disclosure to be in small print. In many cases, it was written in legalese and it was placed not near the information collection area, but rather was accessible on a link contained on the first page of the site. We had also recommended last year that whenever possible that disclosure be audible to the child and in no case did we ever find that to be the case now. While we didn't find adequate disclosure for children and their parents, we did find lots of other kinds of disclosure . . . . particularly on limitations on liability.").

[278] More recently my cable company republished its privacy notice in a brochure titled "Your Cable Equipment and Services". The brochure runs twenty pages, and the privacy notice--the last item in the booklet--begins on page 17 and concludes on page twenty. The brochure arrived in an envelope with a bill and pay-per-view listings. The privacy notice is preceded in the text by sections headed "Credit for Service Outage," "Complaint Procedures for Non-Billing Disputes," and "Employee Identification."

the merchant truly wishes to be to those who do not want their names sold to third parties. [279] One study of information disclosure to consumers found disclosures to be most useful when the consumer "(a) has easy access to the information at the point of sale, (b) can readily comprehend and process the information, and (c) can use it to make direct comparisons of the choice alternatives among relative attributes--in short, when the information is easy to use and relevant to the choice process."[280] My cable company's notice fails that test.

Of course, not all merchants behave in such a fashion. Some take steps to increase the likelihood that their message will be read and responded to by those who object to the selling of their names. For example, the American Bar Association makes the following statement to members in its census form: "On occasion, the ABA makes its list of names and addresses available to carefully screened companies for a rental fee. However, if you prefer not to receive information, please call [toll free number] or mark here." The form then contains an oval which members can mark and return to the ABA along with their answers to other queries on the form. In comparing the two forms, it may be relevant that the ABA is a non-profit organization operated at least in part for the benefit of its members. [281]

---

[279] *See also* Judith Waldrop, *The Business of Privacy*, American Demographics, Oct. 1994, at 46, 48 (quoting Georgetown University professor Mary Culnan, as citing statement made at DMA spring 1994 meeting that "fifty percent of catalogers don't give their customers a convenient way to remove their names from the company's list.").

[280] George S. Day, *Assessing the Effects of Information Disclosure Requirements*, J. Mktg., April 1976, at 42, 47. *See also* William J. Eskridge, Jr., *One Hundred Years of Ineptitude: The Need for Mortgage Rules Consonant with the Economic and Psychological Dynamics of the Home Sale and Loan Transaction*, 70 Va. L.Rev. 1083, 1163-64 (1984).

[281] Though the ABA form is a substantial improvement over the cable company Notice, it is still subject to criticism. The notice appears at the end of a two-page form. Unlike other questions on the form, it is not numbered, and so readers short on time (and what lawyer is not) may not realize immediately that it calls for a decision.

Another model comes from a form which is the product of an agreement between the American Express Company and the New York Attorney General's Office. In 1992, they entered into an Agreement of Voluntary Assurances under which American Express agreed to notify its cardmembers "in a clear, conspicuous and understandable manner" in a form of at least ten point type, with a heading that was printed either in boldface or a different color from the remainder of the notice, that they had a right to opt-out of American Express mailing lists by writing or calling a toll-free number. A copy of the agreement is available at *American Express/New York Attorney General Agreement Announced,* PR Newswire, May 13, 1992.

An opt-out system like the one used by my cable company is likely to be less than effective in matching people up with their preferences. That is to say, it will probably produce a result in which many people who do not wish to receive solicitations receive them, and in which personal information is sold about many people who would prefer it not to be sold. That is so because the availability of an opt-out mechanism is obscured and the mechanism itself is not easily used. As long as marketers have the power and incentive to inflate strategic transaction costs, the market is unlikely to produce an efficient equilibrium.

3. Consumer Limitations.

A third explanation for th e failure of consumers to opt out as often as their answers to the surveys might suggest lies in the consumers themselves. An 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. [282] In this context, that might translate into a failure to add their names to opt-out lists.

It may be that the appropriate response to that is to ignore it: in theory, consumers will act to take themselves off lists if their privacy matters more to them than the cost of having their names removed. Consumers who don't act are making a statement that their privacy is not worth very much to them. If it is not worth very much to most consumers, then perhaps society would be better off focusing on other concerns which do matter to consumers.

But the theory overlooks the reality that consumers act inconsistently with their preferences. Why do consumers do that? E. Scott Maynes has argued that consumers suffer from handicaps in dealing with business, handicaps that contribute to asymmetries in consumer-

[282] The field has its own journal, the Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior. A bibliography updating scholarship in this field was published in the Journal in 1993 and contained 1700 entries. 6 J. Consumer Satisfaction, Dissatisfaction and Complaining Behavior 217 (1993). The leading article is Arthur Best & Alan R. Andreasen, *Consumer Response to Unsatisfactory Purchases: A Survey of Perceiving Defects, Voicing Complaints, and Obtaining Redress*, 11 L. & Soc. Rev. 701 712 (1977) (only 30.7% of consumers perceiving problems voice complaints).

business relationships. [283] The first handicap, according to Maynes, is that "a person's interest as a consumer is always secondary to one's producer interest in a job-profession-business, at least until retirement." [284] Consequently, "many consumers cannot find the time to manage effectively consumption that has grown more complex and dynamic." [285]

The second handicap arises from the capacity of merchants to focus on a particular task while consumers must simultaneously grapple with numerous decisions. Maynes has written that as a producer, "a person is concerned with a single job, product, or industry. As consumer, by contrast, one's interest is spread thinly across thousands of transactions and the management of hundreds of possessions."[286] Thus, the consumer is an "amateur-generalist" dealing with an expert. While Maynes may overstate the point--businesses surely must deal with many transactions too--businesses have the capacity to hire specialists to deal with particular matters in a way that few consumers can match.

The opt-out situation may be compared to what is sometimes called "negative-option billing." Negative-option billing is familiar to many consumers from book and music clubs. Typically, from time to time members of the book club receive a brochure describing the club's offerings. If members do not respond by a particular date, the books are automatically sent to them. Members who do not wish to receive the books must mail a notice to that effect to the

---

[283] E. Scott Maynes, *Consumer Problems in Market Economies* in *Encyclopedia of the Consumer Movement* 158-59 (Stephen Brobeck, ed. 1997)

[284] E. Scott Maynes, *Consumer Problems in Market Economies* in *Encyclopedia of the Consumer Movement* 158 (Stephen Brobeck, ed. 1997).

[285] E. Scott Maynes, *Consumer Problems in Market Economies* in *Encyclopedia of the Consumer Movement* 163 (Stephen Brobeck, ed. 1997). *Cf.* Howard Latin, *"Good" Warnings, Bad Products, and Cognitive Limitations,* 41 UCLA L. Rev. 1193, 1216 (1994) ("Once it is recognized that decisionmaking capacities are limited and that people have many competing demands made on their time and attention, the failure of consumers to read some product warnings becomes foreseeable and inevitable.").

[286] E. Scott Maynes, *Consumer Problems in Market Economies* in *Encyclopedia of the Consumer Movement* 158-59 (Stephen Brobeck, ed. 1997).

club.[287]

Whether purchases are to be made by negative-option or positive-option has a significant effect on consumer purchases. As one consumer attorney has written, "[a]s a result of such negative-option offerings, many families have acquired an abundance of unwanted items because they failed to return a card within a stated time period." [288] Though there is little publicly-available empirical evidence on what effect negative options have on consumer choice--as distinct from positive options--what is available shows rather emphatically that it makes a significant difference. Thus, the Federal Communications Commission studied how consumers responded to offers to "unbundle" services by telephone companies. The FCC found that consumers who had to indicate affirmatively that they wished to purchase the optional maintenance plan subscribed about 44% of the time. Consumers who could subscribe by doing nothing--that is, through a negative option--subscribed 80.5% of the time--for a difference of about 36% of the consumers.[289]

Similar results have shown up in the cable television industry. In Canada, cable television companies found that when new channels are offered in normal ways, only 25% of customers subscribe, but when made available through negative options, 60 to 70% of the subscribers do not reject the offer.[290] In other words, for many cable customers, the key factor in

---

[287] Negative-option purchases are regulated by the FTC. *See* 16 C.F.R. § 425.1.

[288] Bruce Craig, *Negative-Option Billing; Understanding the Stealth Scams of the '90s*, 7 Loyola Consumer L. Rptr. 5, 6 (1994). *See also* Meg Cox, *For the Nation's Troubled Book Clubs, Main Selection of This Year is Change*, Wall St. J., July 24, 1992 at B1 ("receiving mail selections [members] don't want but have forgotten to cancel is one of the most annoying aspects of book clubs.).

[289] Federal Communications Commission, *Inside Wire Survey* (July 18, 1988). The FCC study is no longer available, but is discussed in Dennis D. Lamont, Comment, *Negative Option Offers in Consumer Service Contracts: A Principled Reconciliation of Commerce and Consumer Protection*, 42 U.C.L.A L.Rev. 1315, 1330-31 (1995). The FCC examined 50 cases of positive option offers and 22 cases of negative option offers. *See also* Owen R. Phillips, *Negative Option Contracts and Consumer Switching Costs*, 60 Southern Economic J. 304, 305 (1993) (writing of inside wire maintenance, "under a negative option . . . in the Rocky Mountain region, about 75% of the customers did not deny the service and so received it. In the Northwest where a positive option was required to begin the service, about 75% of the telephone customers did not respond and so did not receive it.").

[290] *See* William Walker, *NDP Set to Ban Negative Option Billing*, Toronto Star, Feb. 24, 1995 at A3. *See*

the purchasing decision is not the cost or content of the programming, but rather whether they have to act.

Merchandisers have acknowledged th at consumers buy more readily when items are sold through negative options. For example, when one cable television provider switched its offering of a new channel from a negative option to a positive option, the company reduced its estimate of the number of expected subscribers to the new channel from 80 percent to 50 percent. [291] Similarly, when the FTC took testimony on negative option selling, it noted that "several industry members quite candidly admitted that if a positive option were offered, subscribers would buy proffered merchandise at a lower rate of purchasing." [292]

No one suggests that consumers would respond to all negative option offerings equally. To take a fanciful example, if a business supplied a service and stated that it would charge $20,000 unless the consumer sent in a form, in which case the service would cost $10, virtually every consumer who purchased the service would surely send in the form. But privacy seems less like that example, and more like the book that consumers buy but never read, simply because it is easier not to send in the form. One observer has noted that consumers are more likely to make a purchase through a negative-option plan if they don't notice that they are making the

---

also Robert Brehl, *Rogers TV Woes Don't Hit Shares*, Toronto Star, Jan. 7, 1995, at C2 (cable company forecast "dramatically" fewer subscribers if negative option not used); Ian Austen, *Rogers Demands Dismantling of Stentor*, Calgary Herald, Jan. 27, 1995, at D14 (cable company official predicts lower number of subscribers unless negative option used).

[291] Bruce Craig, *Negative-Option Billing; Understanding the Stealth Scams of the '90s*, 7 Loyola Consumer L. Rptr. 5 (1994); Kathy Clayton, *Subs to TCI: We Want Our $1 Encore*, Cable World, July 1, 1991, at 1, 20.

[292] FTC, Statement of Basis and Purpose for Trade Regulation Rule, Use of Negative Option Plans by Sellers in Commerce, 38 Fed. Reg. 4896, 4902 (1973). The Statement cautions, however, that "Some of these same parties stated that such an assumption was based on opinion since they had never fully operated a positive option statement." The Commission declined to find that negative option selling "is inherently unfair in that it relies, in substantial part, on exploitation of subscribers' natural preoccupations with or diversions to more important or pressing personal affairs, and on traits of human character such as procrastination or forgetfulness in order to impose liability upon subscribers for merchandise which subscribers may not want and have taken no affirmative steps to obtain." In so doing, the Commission took into account the claims of industry representatives that consumers joining book and record clubs were familiar with club procedures. *Id.* at 4902-03.

purchase.[293] In particular, inexpensive items and services are more likely to be overlooked: "even if the consumer happens to notice the charge, he or she might not devote much attention to it because of the time and effort to determine the cause of the charge and to have it removed from the bill. Moreover, those in vulnerable positions, such as the elderly or foreign born persons, might feel intimidated or deterred from objecting to the charge." [294] Obviously, a system in which people can be said to make purchases that do not reflect their preferences is inefficient.

The analogy to negative options seems clear: many consumers are troubled enough about solicitations to have written to marketers to opt out; as to them, the current default rule does not much matter. Still others would like to continue receiving solicitations, and so they are not troubled by the current default, though a change in that default might make them unhappy. But a third group will not act to change the default setting to one that more closely reflects their preferences. To put it bluntly: for many consumers, default rules matter. They affect choices.

In sum, in light of all these obstacles, surely consumers can be forgiven for abandoning efforts to have their names removed, as indeed some have. [295] But all of this leads to a troubling conclusion: namely, that existing commercial practices and laws frustrate consumers in accommodating their preferences. Can that be fixed so that consumers can attain their goals without unduly burdening business? The article now turns to that question.

V. Fixing the Problem

---

[293] Bruce Craig, *Negative-Option Billing; Understanding the Stealth Scams of the '90s*, 7 Loyola Consumer L. Rptr. 5, 8 (1994).

[294] Bruce Craig, *Negative-Option Billing; Understanding the Stealth Scams of the '90s*, 7 Loyola Consumer L. Rptr. 5, 8 (1994):

> If a merchant configures a negative-option offering that remains below consumer and enforcement levels of concern, and if that offering is made to a large customer base that will be billed regularly, negative-option billing has the potential to provide substantial additional income to the billing merchant.

[295] William M. Bulkeley, *Congress's 'Cure' for Junk Calls Runs into Skepticism at the FCC*, Wall St. J., May 19, 1992 at B6 (many consumers on Florida's "Don't Call" list continue to receive so many unsolicited calls that they drop off the list).

An approach that produced an efficient outcome that genuinely reflected consumer preferences would require consumers to be better informed than they are at present; eliminate unnecessary transaction costs; and tear down unnecessary barriers to consumers acting in accordance with their preferences. As discussed above, we do not have that today: consumers often find it difficult to opt-out, and it appears that businesses have an incentive to make it that way, as well as the power to make it more expensive for consumers to opt out. How could we change to a system in which that is not so?

A. A Voluntary System

One option is for businesses to move voluntarily to an opt-out system, free of government regulation--except perhaps government enforcement of broken promises. Surveys have generally shown that consumers prefer voluntary privacy policies to legislation (though if companies fail to adopt appropriate privacy policies, consumers would support changes in existing law). [296]

Some reasons exist to think that may happen. Many trade guidelines already call upon businesses to provide notice of their information policies and allow consumers to opt-out. [297]

---

[296] Alan F. Westin, *"Whatever Works" The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues* in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F> (in 1995, 72% of public preferred good voluntary privacy policies by business, if those are provided, over legislation; in 1997, 70% of survey respondents favored voluntary privacy policies over government regulation but 58% of survey respondents wanted legislation to protect online privacy now); Alan F. Westin & Danielle Maurici, *E-Commerce & Privacy: What Net Users Want* 34 (1998) (79% of computer users, 80% of internet users and 76% of internet purchasers prefer privacy self-regulation to government regulation of the internet, and feel that government should regulate only if self-regulation fails).

[297] *See, e.g.* Banking Industry Technology Secretariat, The Bankers Roundtable, *Privacy Principles Implementation Plan* 2; Direct Marketing Association, *Direct Marketing Association Guidelines for Ethical Business Practice* 13; Letter from Kerry C. Stackpole, President & Chief Executive Officer, Electronic Messaging Association, to Robert Pitofsky, Chair, FTC, dated March 31, 1998, concerning Electronic Messaging Association Guidelines; Interactive Services Association, *Principles on Notice and Choice Procedures for OnLine Information Collection and Distribution by OnLine Operators*; Letter from Donald D. Kummerfeld, President, Magazine Publishers of America, to Donald Clark, Secretary, FTC, dated March 31, 1998, concerning information guidelines; Smart Card Forum, *Guide to Responsible Consumer Information Practices*. Each of these documents is available in appendix E to FTC, *Privacy OnLine: A Report to Congress* (1998), and the FTC discussed them at page 15 of that Report. *See also* Evan Hendricks, *Bankers Issue 'Best Practices' Guidelines for Customer Data*, Privacy Times, Dec. 17, 1996 at 4 (Consumer Bankers Association guidelines); Evan Hendricks, *Advertisers Unveil 'Goals' for Electronic Privacy*, Privacy Times, Feb. 15, 1996, at 3 (Coalition for Advertising Supported Information and

Beginning July, 1999, DMA members will have to notify consumers of their information practices and permit consumers to opt-out.[298] The DMA is also developing a list of those who do not wish to receive unsolicited commercial e-mail, similar to its existing lists of those who object to mail and telephone solicitations. [299]

Progress has also been made in preserving privacy on the internet. Recently a number of corporations and associations, under the aegis of the OnLine Privacy Alliance, adopted guidelines for online privacy policies. [300] One third-party oversight privacy program, TRUSTe, claims that one-quarter of all time spent on the internet is spent on sites licensed by TRUSTe. [301] The Better Business Bureau is also establishing a self-regulatory program. [302]

Moreover, the information industry has proved willing to negotiate. Thus, in December, 1997, the FTC reached an agreement with fourteen businesses to limit the sale of certain information, such as social security numbers and mothers' maiden names. Under the agreement, the information could continue to be sold to "qualified subscribers," like investigators, insurers,

---

Entertainment, including American Association of Advertising Agencies and Association of National Advertisers).

[298] *Direct Markets Announce New Guidelines,* Wash. Post, Oct. 16, 1997, at C3. The DMA had previously taken the position that marketers should notify consumers of the uses to which their information might be put and provide an opportunity to opt out. U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 23-24 (1995).

[299] Hearings before the H. Com. on Commerce, Subcomm. on Telecommunication, Trade, & Consumer Protection, *Protecting Consumers Against Cramming and Spamming* (Sept. 28, 1998) (Testimony of Jerry Cerasale, Senior Vice President, Direct Marketing Association), available at <http://com-notes.house.gov/cchear> (last checked Oct. 16, 1998).

[300] Robert O'Harrow, Jr., *Firms Prepare Plan for Protecting Privacy on Internet,* Wash. Post, June 20, 1998, at D3; Jeri Clausing, *Group Proposes Voluntary Guidelines for Internet Privacy,* NY Times, July 21, 1998. The Alliance's website is at <http://www.privacyalliance.org>.

[301] *Industry Hopes Seal-of-Approval Programs will Meet Privacy Self-Regulation Challenge,* 67 U.S.L.W. 2396, 2397 (Jan. 12, 1999) (424 sites licensed by TRUSTe, including all major internet portal sites and 45 of top 100 internet sites; to qualify for TRUSTe seal, web site must display privacy policy, notify consumers what information is collected, who is collecting it, how information will be used, insure security of personal information, and provide mechanism for correcting errors). TRUSTe's web site is at **Error! Reference source not found.**. TRUSTe was recently criticized by privacy advocates for failing to pursue an audit of Microsoft, one of its biggest donors, after Microsoft was accused of collecting consumer data surreptitiously. TRUSTe did scold Microsoft. Jeri Clausing, *On-Line Privacy Group Decides not to Pursue Microsoft Case,* N.Y. Times, March 23, 1999, at C5.

[302] *Industry Hopes Seal-of-Approval Programs will Meet Privacy Self-Regulation Challenge,* 67 U.S.L.W. 2396, 2397 (Jan. 12, 1999). The Better Business Bureau's OnLine program web site is **Error! Reference source not found.**

and lawyers.[303]

But pessimism about the willingness of the information industry to adopt a consumer consent system seems more justified. Critics of the information industry complain that self-regulation has not been effective.[304] The reported failure of half of DMA's membership to use DMA's mail preference service lends credence to such claims.[305]

Commentators have charged that the DMA Code of Fair Information Practices "is not

---

[303] *See* Evan Hendricks, *FTC-Industry Pact: Major Step Forward, Or Deal with the Devil?* Privacy Times, Jan. 2, 1997, at 1, 2.

[304] *See, e.g.*, Public Workshop on Consumer Information Privacy, Session One: Database Study, at 188 (June 10, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Beth Givens, Project Director, Privacy Rights Clearinghouse) ("self-regulatory schemes are the emperor's new clothes. I don't think they work. I don't think the incentives are there for a full and meaningful system of . . . fair information principles to be applied."); *id.*, at 319 (remarks of Evan Hendricks, Editor/Publisher of Privacy Times) ("There has been a long history of failure of self-regulation meeting privacy concerns in this country going back to . . . late 1970s."); *id.*, Session Two, Consumer OnLine Privacy 152 (June 11, 1997) (remarks of Russ Smith, publisher, consumer-info.org) ("I would like to discuss self-regulation, and I would like to find out where it exists. I have not been able to find it over the last few years. I have submitted complaints to numerous industry groups, including the Direct Marketing Association's Ethics Council, and I get no response whatsoever."); *id.* at 175 (remarks of Jean Ann Fox, Director of Consumer Protection, Consumer Federation of America & Vice President, Board of Directors, Consumers Union) ("self-regulatory efforts and voluntary guidelines are very positive and useful, but not sufficient. There are always bad actors that don't comply with the best efforts of the leaders in the industry . . . ."): *id.*, at 188 (remarks of Leslie L. Byrne, Director, U.S. Office of Consumer Affairs) ("I am not convinced that self-regulatory schemes do much in terms of enforcement or anything other than give appearance of doing something to hold the wolves from the door."); Mary J. Culnan, *Self-Regulation on the Electronic Frontier: Implications for Public Policy*, in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F> (arguing that self-regulation has been ineffective because the rules have not been applied equally to all firms within the industry and because data compilers do not have direct contact with consumers); Shelley Pasnik & Mary Ellen R. Fise, *Children's Privacy and the GII*, in same publication ("It is clear that industry self-regulation does not provide adequate protection for children's privacy."); Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C.L. Rev. 847, 874 (1998) ("the presence of great diversity in [the online] industry makes universal participation [by marketers] unlikely. . . .Given the great diversity of companies, a significant number . . . are unlikely to agree on a uniform set of guidelines."); U.S. Sen. Com. on Commerce, Science, and Transportation, Subcom on Communications, *Hearings on S.2326, Children's Online Privacy Protection Act of 1998* (Sept. 23, 1998) available at http://www.senate.gov/~commerce/press/105-287.htm (last checked Oct. 30, 1998)(Testimony of Kathryn Montgomery, President, Center for Media Education) ("A trade association that is financed by its members has little incentive to expel a member who violates stated privacy policies. In addition, when consumers access sites online, they have no knowledge of how that company is viewed by its peers. Similarly, the absence of a certifying seal is too subtle a means of educating Internet users . . . ."); Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 217 (1996). *But see* Robert J. Posch, Jr., *Keep the Privacy Debate in Context*, Direct Marketing, May 1, 1997 (DMA's self-regulation "has always proved successful."); Fred H. Cate, *Privacy in the Information Age* 108 (1997) (arguing that critiques are misplaced and fail to reflect recent successes of self-help model); Lisa Rosenthal, *The IRSG Principles: A Promising Self-Regulatory Program to Curb Misuse of Non-Public SSNs*, 19 At Home With Consumers, No. 1 at 3 (May 1998) ("self-regulation is more prompt, flexible, and effective than government regulation [and] can bring the accumulated judgment and experience of an industry to bear on issues that may be difficult for the government to define with bright-line rules.").

[305] See *supra* note ___ and accompanying text.

systematically honored by companies engaged in direct marketing activities." [306] Nor does the DMA maintain data on compliance with its Code: [307] indeed, it has been reported that the DMA did not make a public inquiry after one of its members, in the wake of an investigation by the attorneys general of fourteen states into its mailing practices, agreed to change its practices and pay a $400,000 settlement.[308] Members of the DMA's Privacy Task Force themselves are said to ignore DMA guidelines; [309] in fact, a representative of the company which entered into the $400,000 settlement chaired the DMA Privacy Task Force.[310] Moreover, even if all DMA members comply with DMA guidelines, there will still be direct marketers who are not bound by DMA rules because they are not DMA members.

Similarly, with respect to internet sites, the FTC has concluded that an effective self-regulatory system has not emerged.[311] When the Electronic Privacy Information Center ("EPIC") studied web sites of new DMA members, it found that only eight out of forty had any form of privacy policy, and of these only three had privacy policies that satisfied DMA

---

[306] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 217 (1996).

[307] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 217 (1996).

[308] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 338-39 (1996). *See also* FTC, Public Workshop on Consumer Information Privacy, Session One: Database Study, at 288 (June 10, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Robert Biggerstaff) ("I know people personally who have followed up with complaints and complained time and time again and are basically told eventually that DMA doesn't take any action against their people, they have no ability to take any action against their members . . . ."). *But see* Supplemental Comments of the Direct Marketing Association, Inc. Before the Federal Trade Commission (July 16, 1997) available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/dma027a.htm> (last checked Aug. 21, 1998) (DMA will refer non-complying members to DMA Committee on Ethical Business Practice which publishes compilation of cases it reviews).

[309] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 309 (1996).

[310] Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 338-39 (1996).

[311] Federal Trade Commission, *Privacy OnLine: A Report to Congress* 41 (1998). *See also* Statement of the FTC on Consumer Privacy on the World Wide Web Before the Subcom. on Telecommunications, Trade and Consumer Protection of the H. Com. on Commerce, July 21, 1998, available at <http://www.ftc.gov/os/9807/privac98.htm> (last checked July 30, 1998). (Our March 1998 survey . . . revealed that, at the time of the survey, the state of self-regulation was inadequate and disappointing."). For discussion of the relative merits of self-regulation, compared with government regulation, or market forces, in the privacy context, see Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, in NTIA, *Privacy and Self-Regulation in the Information Age*, available on internet at <http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1F>.

requirements.[312] Even a DMA official has acknowledged that "we clearly have a way to go."[313]

Privacy Times reports that at least one look-up service, Infotel, has refused to abide by the December, 1997 FTC agreement. Infotel provides assistance in locating people and conducting background checks, such as one service, "Checkmate," that allows people to investigate their dates.[314] And one member of the OnLine Privacy Alliance has already been accused by the FTC of misrepresenting the uses for which it collected data: the matter terminated in a settlement in which the company did not admit wrongdoing.[315]

Even more troubling is the failure of the information industry to comply with existing laws, let alone non-binding industry guidelines. For example, when a trade magazine wrote to 48 telemarketers requesting copies of their "Do Not Call" policies--which telemarketers are required to provide upon request[316]--only seventeen of the telemarketers had responded after three months.[317]

Accordingly, if the information industry as a whole is to adopt a consumer consent regimen, government intervention is likely to be needed. Government intervention could take one of two forms. I now discuss them.

B. A Mandated Opt-Out System

One solution would preserve the default that businesses could trade in consumer information if consumers take no action but establish mechanisms both to insure that consumers

---

[312] EPIC, *Surfer Beware II: Notice is not Enough* (June 1998) (available on web at www.epic.org).

[313] EPIC, *Surfer Beware II: Notice is not Enough* (June 1998) (available on web at www.epic.org) (quoting DMA's Vice President of Consumer Affairs, Patricia Faley).

[314] Evan Hendricks, *Look-Up Service Spokesman Doubts Efficacy of FTC-Industry Agreement,* Privacy Times, March 6, 1998 at 1, 2.

[315] *See* Evan Hendricks, *FTC, GeoCities Settle Internet Privacy Case,* Privacy Times, Aug. 14, 1998, at 2-3; *In re GeoCities,* FTC File No. 9823015 (1998). The consent decree can be found at <http://www.ftc.gov/os/1998/9808/geo-ord.htm> (last checked Sept. 24, 1998).

[316] *See* 47 C.F.R. § 64.1200(e)(2).

[317] Evan Hendricks, *Telemarketers Accused of Ignoring Junk Phone Law,* Privacy Times, June 12, 1998, at 5-6.

are informed about the choices available to them and also to eliminate unnecessary transaction costs. For example, such a rule could specify the terms of notices to consumers so that notices would be readily comprehensible and likely to be read. A "clear and conspicuous" standard could be employed to prevent companies from obscuring the information. [318] Consumer law is filled with required notices; [319] another could be drafted. Companies could be required to maintain toll-free numbers for opt out calls.

But such notices have a downside. First, they tend to suffer from some of the same deficiencies as the cable company's Privacy Notice: they often contain dryly legalistic, uninteresting prose. Required notices always raise a question about whether consumers actually read them, just as with the Privacy Notice. Moreover, the history of required notices is a checkered one: though some mandated notices seem to have have aided consumers, [320] some commentators are less sanguine about their utility. [321] The discussion above of the Fair Credit Reporting Act opt out--the Acting Comptroller of the Currency observed that few consumers recall seeing the opt-out forms, which are required to be clear and conspicuous --suggests that when businesses do not want consumers to see a notice, consumers won't.[322]

The Truth in Lending Act offers a further cautionary tale. When first enacted in 1968, Truth in Lending required lenders to provide consumers with a complex set of disclosures. [323]

---

[318] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 Stanford L. Rev. 1193, 1272 (1998) (suggesting clear and conspicuous standard).

[319] *See, e.g.*, FTC Regulations Holder-in-Due-Course Regulation, 16 C.F.R. § 433.2; Truth in Lending Rescission Regulation, 12 C.F.R. § 226.15(b).

[320] *See, e.g.*, Michael J. Wisdom, Note, *An Empirical Study of the Magnuson-Moss Warranty Act*, 31 Stan. L. Rev. 1117, 1145 (1979); Jacqueline Schmitt, et al., *Impact Report on the Magnuson-Moss Warranty Act* 16, 18, 19 (1980); Arthur Young & Co., *Warranties Rules Warranty Content Analysis* 36 1979).

[321] *See generally* William C. Whitford, *The Functions of Disclosure Regulation in Consumer Transactions,* 1973 Wisc. L. Rev. 400; Robert L. Jordan & William D. Warren, *Disclosure of Finance Charges: A Rationale,* 64 Mich. L. Rev. 1285, 1320-22 (1966); Homer Kripke, *Gesture and Reality in Consumer Credit Reform,* 44 N.Y.U. L.Rev. 1, 5-8 (1969). *See also supra* note ___ and accompanying text.

[322] *See supra* notes ___ and accompanying text.

[323] Pub. L. No. 90-321, 82 Stat. 146 (1968), codified as amended at 15 U.S.C. § 1601 et seq.

Ambiguities in the statute and its implementing regulations led to more than 1,500 interpretations by 1980, as well as numerous lawsuits, often over technical questions. [324] Though the statute undoubtedly improved the manner in which information was provided to consumers, it also required that information be presented in a format many found confusing. [325] In 1980, Congress enacted the Truth in Lending Simplification and Reform Act, in large measure to fix problems with the original statute. [326] Though disclosures about information policies are likely to be less complex than disclosures about credit, the history of Truth in Lending suggests that disclosure requirements are not always a perfect solution to a problem, at least not as initially created. In addition, it raises questions about the competence of government to draft useful notices.

A second problem with a regulated opt-out system is that some enforcement apparatus would have to be maintained to insure that businesses were living up to their obligations under the regulation. [327] As discussed above, many marketers have not lived up to their own industry guidelines and questions have been raised about whether marketers are in compliance with existing law. [328]

Third, opt-out systems do not provide businesses with an incentive to help consumers act in accordance with their preferences. Consequently, additional regulation might be required to insure that businesses provided consumers enough information to make informed decisions.

C. A Mandated Opt-In System

It remains to consider an opt-in system, with a default rule different from the one

---

[324] Michael M. Greenfield, *Consumer Law* 229 (1995) Dee Pridgen, *Consumer Credit and the Law* § 4.01 at 4-2 (1996).

[325] *See, e.g.*, Dee Pridgen, *Consumer Credit and the Law* § 4.01 at 4-1-4-2 (1996)("the disclosures were overly burdensome to creditors and too cumbersome to be of much use to the average consumer.").

[326] Pub. L. No. 96-221, 94 Stat. 168 (1980). *See generally* Rohner, *Truth in Lending "Simplified": Simplified?* 56 NYU L.Rev. 999 (1981).

[327] Some enforcement apparatus would also be needed for an opt-in system, if one were to be adopted.

[328] See *supra* notes --- and accompanying text.

established by today's system.[329] Obviously, businesses and consumers who do not value privacy are likely to prefer an opt-out system, while privacy advocates can be expected to favor an opt-in system.[330]

1. The Effect of an Opt-In System on Transaction Costs

One goal in fashioning rules is to minimize transaction costs. That is especially important in consumer transactions, because the stakes involved are generally so low that large transaction costs may exceed the value of the transaction and make the transaction uneconomic.

While some transaction costs are inevitable in any system in which consumers can opt out or opt in, some transaction costs can be avoided. In particular, strategic behavior costs can be avoided by using a system which discourages parties from generating such costs. As discussed above, the system in which we operate at present encourages businesses to inflate strategic behavior costs because the businesses increase their own gains, albeit at the expense both of the 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 them. Instead of the opt-out situation in which merchants were obliged to provide a message they did not wish the consumer to receive, in an opt-in regime we would see merchants' efforts

---

[329] "Default rules fill the gaps in incomplete contracts; they govern unless the parties contract around them." Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale. L. J. 87, 87 (1989). *See* also W. David Slawson, *The Futile Search for Principles for Default Rules*, 3 S. Cal. Interdis. L.J. 29, 29 (1993) ("Default rule analysts call a law a default rule if a contract could preempt it."). For the argument that opt-in rules do not fall afoul of the First Amendment, see Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1277-82 (1998). *See generally* Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 Cornell L. Rev. 1756(1995). *See also* Jonathan Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 Tex. L. Rev. 1395, 1434-38 (1987) (arguing that privacy legislation would not violate First Amendment).

[330] In the online context, it may soon be possible for the consumer to set the default. Internet browsers are currently in development which would permit the consumer to identify his or her privacy preferences. *See* Federal Trade Commission, *Privacy OnLine: A Report to Congress* 9, 50, N.Y.2d. 44, 45 (1998). That may be helpful to consumers who are technologically savvy enough to take advantage of that option--and who possess up-to-date browsers--but will obviously be of little aid to consumers making purchases through means other than the internet.

harnessed to providing a message they want the consumer to receive. [331]

How do we know that companies would behave in such a way if they could not use consumer information without consumer consent? We do have some information about how companies behave in an opt-in environment. After the Federal Communications Commission, in interpreting the Telecommunications Act of 1996, ruled that phone companies seeking to use phone calling patterns for marketing purposes must first obtain the consumer's permission, [332] the telephone company in my area attempted to secure that permission. Its representatives called and sent mailings to subscribers. The company also set up a toll-free number for consumers with questions. The mailing I received is brief, attractively printed in different colors, and written in plain English. It also promises, in words which are underlined that "we'll never share this information with any outside company. . . ." A postage paid envelope and a printed form is included for consumers to respond. Consumers who accept the offer need only check a box, sign and date the form, and print their name. The company also offered consumers incentives to sign up--such as offering them at various times a $5 check or their choice of two free movie tickets or a certificate worth $10 towards merchandise at certain retailers--thus increasing the likelihood that consumers will pay attention to the information. In sum, the company has done everything it can to eliminate consumer transaction costs.

An opt-in system thus increases the likelihood that consumers will choose according to

---

[331] *Cf.* Howard Beales et al., *The Efficient Regulation of Consumer Information*, 24 J. L. & Econ. 491, 522-23 (1981):

> There is usually an advantage in designing disclosure remedies that leave as large a role as possible to normal market forces, to restrict the market as little as possible. The goal should be not to specify the exact information to be disclosed and the exact manner in which it will be disclosed but to give sellers the proper incentives to make these decisions on their own. This reduces the consequences of a bad decision by the government since it avoids forcing sellers to disclose information in an ineffective manner or to disclose information which, because of a change in circumstances, is no longer desired by consumers. It also increase the effectiveness of the remedy by harnessing sellers' own incentives to develop the most effective ways of informing consumers. Thus, innovation should be encouraged by leaving sellers latitude to experiment.

[332] 63 Fed. Reg. 20,326. *See also* Evan Hendricks, *FCC Backs 'Opt-in' for Phone Cos. Secondary Use of*

their preferences rather than choosing according to the default. That alone offers a significant reason for adopting an opt-in system.

Recall equation (1) in which consumers should buy if $V_P > P +$ (lesser of C_{OO} and V_{LP}), or consumers should buy if the value to the consumer of purchasing the product is greater than the price of the product plus the lesser of the cost of opting out and the value to the consumer of the consumer's privacy. What would the equation look like in the opt-in scenario? The consumer who wishes to preserve his or her privacy would no longer have to take into account the direct costs of doing so, and so the consumer should buy if the value of the product to the consumer exceeds its cost, or simply:

(3) Consumer should buy if $V_P > P$

However, the seller in the opt-in scenario has lost income because seller can no longer sell the consumer's personal information unless the consumer opts in. Hence seller may respond by raising the price, P. But because consumer will buy only if the price is less than the value to the consumer of owning the product, and because seller presumably wants to make sales, seller has an incentive to minimize the price. Consequently, seller not only has no reason to engage in strategic behavior to increase transaction costs, seller instead has an incentive to minimize transaction costs.

It still remains to consider consumers who wish to have their personal information used. As the opt-in transaction can be considered a separate transaction--just as the decision to subscribe to the services my telephone company provides is separate from the decision to allow it to use calling information for marketing purposes--they should also purchase a product if the value of the good exceeds the price. They should then allow the sale of their personal information if the value to them of opting in is greater than the cost of opting in. Because

---

Customer Data, Privacy Times, Feb. 20, 1998, at 4.

businesses will wish consumers to opt in, businesses can be expected to minimize the cost of opting in. Once again, we see that an opt-in system is likely to reduce strategic transaction costs--exactly the opposite of an opt-out system.

An opt-in system also increases the prospect that direct mailing would be tailored to what consumers wish to receive. When companies have a reason to obscure opt-out provisions, as is currently the case, they have no incentive to offer schemes in which consumers could express a desire to receive some solicitations but not others. To return to my personal situation, companies that don't ask me what I would like to receive have no opportunity to learn that I want to receive children's clothing catalogs but not women's clothing catalogs. If, on the other hand, companies have to persuade me to opt in, they have a reason to offer me the opportunity to receive only the kinds of catalogs I wish to receive. At least one company has found that when it offered consumers a variety of options, some consumers who formerly opted out of all solicitations chose instead to receive some, as long as they did not have to receive all. [333]

2. Theory of Default Rules

In recent years, a number of scholars have written about default rules. [334] This attention was triggered in large measure by an important article by Ian Ayres and Robert Gertner. [335] Ayres and Gertner acknowledge that transaction costs should play a role in setting defaults, but they go on to argue that in setting defaults, law-makers should also take into account whether parties fail to contract around defaults for strategic reasons. They contend that in some circumstances, the law should establish "penalty defaults"; that is, defaults which give a party an

---

[333] *See* Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* 181-82 (1997).

[334] *See, e.g., Symposium on Default Rules and Contractual Consent*, 3 S. Cal. Interdisc. L.J. 1-444 (1993).

[335] Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale. L. J. 87 (1989).

incentive to contract around the default rule. [336]

One reason for penalty defaults, according to Ayres and Gertner, is to give more informed contracting parties incentives to disclose information to less informed parties. [337] "By setting the default rule in favor of the uninformed party, the courts induce the informed party to reveal information, and consequently the efficient contract results." [338] Ayres and Gertner argue that otherwise, the more informed party might choose not to disclose the relevant information, even though failure to disclose might lead to an inefficient result, simply because concealing the relevant data might enable the more knowledgeable party to end up with a larger slice of the pie. [339] "When relatively informed parties strategically withhold information, courts, to promote information revelation, should choose a default that the informed party does not want." [340]

Ayres and Gertner's theory of penalty defaults closely fits the sale of information. At present, businesses have little incentive to disclose to consumers how their personal information is used or that they can opt out of its use. That leads to inefficient results. [341] Changing the default gives businesses an incentive to make disclosures and increases the likelihood that an

---

[336] *Id.* at 91.

[337] *Id.* at 97.

[338] *Id.* at 99.

[339] *Id.* at 99-100. Robert E. Scott calls default rules adopted for such reasons "information-forcing defaults." Robert E. Scott, *A Relational Theory of Default Rules for Commercial Contracts,* 19 J. Leg. Studies 597, 609-11 (1990). *See also* Alan Schwartz, *The Default Rule Paradigm and the Limits of Contract Law,* 3 S. Cal. Interdis. L.J. 389, 390-91 (1993):

> let a set of parties, say retailers, understand the commercial subject and the law relevant to it while the other set of parties, say consumers, does not. An information-forcing default rule is chosen because it is unfavorable to sophisticated parties; the new contract the sophisticated parties propose to displace the unfavorable default is supposed to inform the unsophisticated parties of the subject's relevance and of the terms that will govern disputes unless these parties speak up.

[340] Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale. L. J. 87, 103-04 (1989).

[341] In a later article, Ayres and Gertner argued that "the introduction of transaction costs can actually exacerbate the inefficiencies of strategic bargaining--so the gains from contracting can fall by more than the size of the transaction costs." Ian Ayres & Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 Yale L. J. 729, 733 (1992). That suggests that providing businesses both the capacity and an incentive to inflate transaction costs is particularly troublesome.

efficient contract results.[342]

3. Analogies to Negative Option Regulation

Another reason for an opt-in system is that opt-out systems, as discussed above, are analogous to negative options in that agreement is conveyed not by an affirmative manifestation of assent but rather silence. Normally silence does not operate as acceptance of an offer.[343] Similarly, if a party to a contract suggests a change in its terms, the other party's silence does not constitute acceptance--though courts will sometimes infer from conduct a tacit agreement to modify a contract.[344] We do not allow a seller to impose a contract on a buyer through negative options. Why should we allow a seller to impose a term on a buyer through negative options--without even giving notice to the buyer?

Recognizing that negative option agreements are troublesome, Congress and administrative agencies have regulated them in some contexts. Thus, Congress has barred cable operators from charging consumers for services which the consumer "has not affirmatively requested."[345]

In the area in which negative options are probably most used--book and music clubs--their use is regulated by an FTC rule.[346] That rule requires the promotional material "clearly and conspicuously disclose the material terms of the plan," including the fact that the subscriber must

---

[342] For a thoughtful application of Ayres' & Gertner's approach to default rules to privacy in cyberspace, which also comes to the conclusion that the default rule should be opt-in, though using a somewhat different analysis, see Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 Stanford L. Rev. 1193, 1251-59 (1998).

[343] 1 *Corbin on Contracts*, § 3.18, at 402-07 (Joseph M. Perillo 1993); 2 Samuel Williston, *A Treatise on the Law of Contracts* §§ 6:3, 6:49, at 17-18, 561(Richard A. Cord 1991). Some exceptions appear in the Restatement (Second) of Contracts, § 69 (1979).

[344] Corbin *supra* note ___ § 3.18 at 564.

[345] 47 U.S.C. § 543(f). The section also provides that "a subscriber's failure to refuse a cable operator's proposal to provide such service or equipment shall not be deemed to be an affirmative request for such service or equipment." *See also* 47 C.F.R. § 76.981.

[346] 16 C.F.R. Part 425.

notify the seller if the subscriber does not wish to purchase the particular selection. [347] Sellers are also obliged to provide forms to subscribers which "clearly and conspicuously" disclose that the seller will send the subscriber the selection unless the subscriber returns the form to the seller. [348] These book and music clubs are significantly different from the type of negative options used in information practices because the book and music clubs notify the consumers in advance of the nature of the program and the consumer voluntarily joins the club knowing how the club works. It seems anomalous to regulate the clubs--given that consumers choose to join them--but not information practices--given that many consumers are not even aware of how their information will be used and so cannot be said to have knowingly "joined."

4. Internalizing Externalities

The sale of information is troublesome in part because it creates externalities. Sometimes, when a person engages in an activity, the activity imposes costs on others that the person is not required to take into account in deciding whether to pursue the activity. These costs are considered externalities. [349] The feelings experienced by those whose information is sold and used without their knowledge constitute just such externalities. [350] 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--addresses that problem by internalizing the externality. To put it another way, consumers could bar the sale of their information unless they received compensation which they regarded as adequate--something which would compensate them for the feelings they suffer; namely, the externality.

---

[347] 16 C.F.R. § 425.1(a)(1)(i).

[348] 16 C.F.R. § 425.1(a)(2)(ii).

[349] *See* David W. Barnes & Lynn A. Stout, *Cases and Materials on Law and Economics* 23 (1992).

[350] *See* Kenneth C. Laudon, *Markets and Privacy*, 39 Communications of the ACM No. 9 (Sept. 1, 1996) ("The costs of using personal information to invade the privacy of individuals is far lower than the true social cost because part of the cost of invading privacy is borne by the individual whose privacy is invaded.").

Presumably, the business which bought the information would raise the price to others to compensate for any payment to the consumer. Hence, the price would take into account the social costs incurred when the information is sold, and thus the externality would be internalized in the form of the higher price. The higher price might reduce the number of businesses which purchase the information, but because the higher price reflects the true social cost of the sale of the information, it would produce a more efficient equilibrium. [351]

5. Criticisms of Opt-In Systems

Critics of opt-in requirements have argued that consumers cannot predict what solicitations they will want to receive in the future, and so they might choose not to receive information that in fact they would like to have. [352] Consumers would also lose at least some of the benefits they receive from appearing in databases, benefits that were described earlier. [353] But that can be explained to consumers at the time they make the choice whether to receive solicitations. Indeed, an opt-in system gives businesses an incentive to do just that. If consumers, understanding what they are giving up by declining to opt-in, resolutely decide against opting in, that choice should be respected.

Some have argued that an opt-in system would destroy the direct marketing industry

---

[351] An example may make it clearer. Suppose the benefit of adding a particular name to a database is 80 cents, and that the cost to the database company of inputting the data is 20 cents (for typing, electricity, purchasing and maintaining equipment and the like). In that case, if the company is not required to compensate the person whose name is added, the company will make a 60 cent profit by adding the name, and so should do so. But if the cost to the feelings of the individual whose name is added is one dollar--the externality--the addition of the name will lead to a net loss to society of forty cents. That is arrived at by subtracting the gain to the company (60 cents) from the loss to the individual (one dollar). That is not an optimal allocation of resources. On the other hand, if the company is required to pay the person whose name is included in the database one dollar for adding the name--thus internalizing the externality--the company will bear the forty cent loss. A rational company will not wish to incur such a loss and so ought not to add the name. In fact, a company should not add a name to its database unless the value to the company of adding the name exceeds the cost of $1.20. Only when that happens will it be efficient to add a particular name. By making the company bear the costs of increasing the size of its database, as well as obtaining the benefits, society would more readily reach an optimal result.

[352] U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 25 (1995).

[353] *See supra* notes ___ and accompanying text.

because the cost to businesses of having consumers opt in exceeds the value to businesses of consumers opting in.[354] In other words, the argument is that imposing the transaction costs on businesses would make the transactions uneconomic.[355] Is this true? To be sure, each name by itself is not worth very much. Estimates of the value of the worth of individual names are usually expressed in cents, not dollars. For example, a list of 1,000 subscribers to Forbes Magazine goes for $115.[356] Metromail Corp. reportedly charges thirty cents a name for access to its medical

---

[354] *See* G. Bruce Knecht, *Privacy: Junk-Mail Hater Seeks Profits From Sale of His Name*, Wall St. J., Oct. 13, 1995, at B1 (quoting Mary J. Culnan, associate professor at Georgetown Business School as saying "Affirmative assent would kill the direct-marketing industry.").

[355] Judge Posner argues that magazines should be able to sell their subscriber list to other magazines without obtaining the consent of their subscribers for two reasons. *See* Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 398-99 (1978). First, the transaction costs to the magazines of obtaining consent "would be high relative to the value of the list." *Id*. at 398 (1978); *see also* Anthony D'Amato, *Comment*: *Professor Posner's Lecture on Privacy*, 12 Ga. L. Rev. 497, 501 (1978). Second, "the costs of disclosure to the individual are small . . . because the information about the subscribers that is disclosed to the purchaser of the list is trivial; the purchaser cannot use it to impose substantial costs on the subscribers." Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 398-99 (1978); *see also* Anthony D'Amato, *Comment: Professor Posner's Lecture on Privacy*, 12 Ga. L. Rev. 497, 500 (1978) ("I can hardly understand why people complain about getting mail solicitations. A piece of mail does not intrude upon their privacy, and in any event the recipient has the simple alternative of throwing it out without opening it."). Posner explains: "If, therefore, we believe that these lists are generally worth more to the purchasers than being shielded from possible unwanted solicitations is worth to the subscribers, we should assign the property right to the magazine; and the law does this." Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 398 (1978).

I address the issue of the value of the list in light of transaction costs in the following paragraphs in the text. A problem in Judge Posner's reasoning is that it is not demonstrable that the cost to subscribers of disclosure is small. While the subscribers may receive some benefits from the sale of the subscription list--in the form of cheaper subscription rates, because the magazine has another source of revenue, and in receiving solicitations for products that the subscribers might wish to purchase--the survey evidence and other information about consumer preferences discussed above shows that many consumers are troubled by the sale of lists of consumers. *See supra* notes ___ and accompanying text. The difference between what Judge Posner's view would predict and what the surveys and other evidence suggests may possibly be explained by Judge Posner's decision to treat privacy as an intermediate good rather than a good having value in its own right.

[356] Susan Headden, *The Junk Mail Deluge*, U.S. News & World Rep., Dec. 8, 1997. *See also* Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 8 (1997) ("Lists can range in price widely, generally anywhere form $35 to $250 per thousand names."); G. Bruce Knecht, *Privacy: Junk-Mail Hater Seeks Profits From Sale of His Name*, Wall St. J., Oct. 13, 1995, at B1 (in 1995, U.S. News & World Reports charged about eight cents per name, reported to be "about average for magazines with affluent well-educated subscribers"); Paula Crawford Squires, Transactions Go Into a Database; Businesses Compile Dossiers on Customers, Richmond Times Dispatch, July 28, 1996, at A-12 (R.L. Polk & Co., which compiles information provided by consumers when they return product registration cards, maintains a database on some 36 million people. In recent years, it has sold its data for $74 per 1,000 names). The Lotus Marketplace: Households project abandoned after consumer protests, as discussed *supra* note ___ and accompanying text, was to charge $695 for the first 5,000 names and eight cents each for additional names. Anne Wells Branscomb, *Who Owns Information?* 18 (1994).

database of 15 million patients, information useful to pharmaceutical marketers. [357] E-mail addresses are even cheaper.[358]

On the other hand, some marketers seemingly have paid quite a bit more to generate their lists and obtain consumer information. My local telephone company has already been alluded to.[359] But other examples exist. One company has offered free personal computers to consumers who let the company track their activities on the internet and provide the company with detailed personal information. The computers will also display advertisements. [360] Kay-Bee Toy Stores recently offered a five dollar rebate to customers for their names and addresses. [361] Similarly, when R.J. Reynolds wanted a list of smokers for direct advertising purposes, it ran ads in newspapers offering to send free samples or coupons to smokers who wrote in. Philip Morris built a list of about 26 million names--at a cost of distributing 30 million pieces of free merchandise. [362] To be sure, these programs may have provided additional benefits to the companies beyond generating a list of smokers, but they undoubtedly cost much more than a few

---

[357] Kevin DeMarrais, *Big Brother is Watching Your Database*, The Record, Apr. 30, 1995 at A01. Metromail's lists reportedly include sufferers of asthma, diabetes, ulcers, an other illnesses. Susan Headden, *The Junk Mail Deluge*, U.S. News & World Rep., Dec. 8, 1997. Prices may also vary depending on the information provided. For example, one service, which provides lists of college students, charges $40 per thousand names; adding zip codes, class year, and major would increase the cost by a total of $20 per thousand. *See* Gandy, *supra*, note ___ at 91 (1993). Similarly, different occupations are valued differently. Space scientists at $45 per thousand command less than either sociology department heads at $60 per thousand or high school math teachers at $65 per thousand. *See* Gandy, *supra* note ___ at 91. One telephone company charges more for newly-connected customers--$90 or more per thousand-- than for existing customers, at $50 to $55 per thousand. Evan Hendricks, *Bell Virginia's Plan to Sell Customer Names Draws Criticism*, Privacy Times, Aug. 2, 1995, at 4, 5.

[358] Supplemental Comments of Consumer Federation of America to the FTC (June 18, 1997) available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2.ftcpriv2.htm> (last checked Aug. 21, 1998) (one million e-mail addresses available for $89; 30 million e-mail addresses available for $149).

[359] See *supra* note ___ and accompanying text.

[360] Evan Hendricks, *What Price Privacy? Free-PC Has an Offer*, Privacy Times, Feb. 15, 1999 at 3-4. Matt Richtel, *Despite Privacy Concerns, Free PC's Attract Many Consumers and Schools*, N.Y. Times, Feb. 25, 1999, at G7 (more than a million consumers have signed up). The company currently disclaims any intention to sell disclose consumer information to others, but because it can sell advertising on the computers, it can still advertise directly to consumers who accept the offer.

[361] Neil Munro, *Putting a Price on Technology*, 11 Wash. Technology, No. 23, Mar. 6, 1997.

[362] Jonathan Berry, et al, *Database Marketing: A Potent New Tool for Selling*, Bus. Week, Sept. 5, 1994 at 56.

coins for each name generated. [363]

Why would marketers pay more than cents for names given that names are available at such a low price? First, while some lists may be available for only a dime or two per name, those lists may not be useful to the marketers in question. The marketers may be willing to pay quite a bit more for lists that are useful. And second, the prices that list-sellers quote usually focus on the value to the buyer (or renter) of the list for one-time use. The names on the list may be considerably more valuable to the listowner, who can sell (or rent) the names over and over again. A dime per name adds up over multiple sales. Hence, listowners might be willing to pay much more than just pocket change per name to buy the right to use names--perhaps even enough to cover transaction costs and still make a profit.

In addition, a legal regime which required consumers to assent to the use of their names might make the names more valuable. And strategies could be employed to reduce transaction costs. Take magazine subscriptions as an example. Many, probably most, subscriptions are started when the subscriber communicates to the publisher that a subscription is desired. This communication may, for example, take the form of a telephone call, a postcard in a copy bought at a newsstand, or a purchase through one of the magazine sweepstakes companies. In each case, certain information is needed by the publisher to start the subscription--name, address, length of subscription, payment mechanism desired, and the like--and usually the subscriber supplies this information. How expensive would it be if the publisher were also to inquire whether the subscriber would object to including the subscriber's name whenever the magazine's subscription list is sold? [364] A system in which the subscriber granted or withheld permission

[363] *See also* Erik Larson, *The Naked Consumer* 8-9 (1992) ("Recently a swank Boston hotel offered me five bucks to answer a survey. In 1990 American Airlines, citing plummeting cooperation rates, gave survey respondents a $25 travel certificate.").

[364] Judge Posner did note that some magazines seek this information. *See* Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 398, n.13 (1978) ("A few magazines offer the subscriber the option of having his name

when the subscriber initially purchased the subscription and each time the subscriber renewed need not be very expensive.[365]

Would consumers ever opt in under such a system? Little information is available to answer that question. It has been estimated that only five to ten percent of consumers would opt in.[366] On the other hand, America OnLine found that when it enabled consumers to opt-out, more than eighty percent of the people who went to the opt-out area did not opt out but rather asked that they be put on more lists.[367] And obviously, many consumers have reacted to direct marketing offers by buying the product offered, suggesting that they value some offers.

Indeed, some consumers have opted in even in a climate in which consumer information is freely available. One company operates an opt-in e-mail system in which consumers can ask to be added to any of 3,000 different mailing lists. Three million consumers have given their e-mail addresses to that service.[368] The service seems to work: one of its clients increased its sales by

---

removed from the list of subscribers that is sold to other magazines. But this solution is unsatisfactory to the subscribers (presumably the vast majority) who are not averse to all magazine subscriptions.").

The cost of obtaining the consumer's permission might be greater when the subscription is started without a communication from the subscriber to the publisher, as sometimes happens. For example, after I purchased some children's clothing for my daughters from a catalog company, the company ordered a subscription to a parenting magazine for me, presumably to induce me to continue buying their products. I never communicated with the publisher; in time, the subscription lapsed. A legal rule which prohibited the publisher from selling my name without my permission would require a publisher which desired to obtain such permission to convey separately to me a wish to have such permission, in addition to my sending back my consent. That would increase the cost of using my name, but probably not by very much, and in any event such gift subscriptions are probably not common enough to justify taking them into account in formulating privacy rules.

[365] *Cf.* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 Tex. L. Rev. 1, 24 (1997) (arguing in a discussion of businesses that collect data in membership applications "and provide an opportunity to decline outside use of these data" that "the transaction costs for all the parties are minor whether viewed at the moment of *negotiating* the agreement (the ex ante costs) or *complying* with it (the ex post costs).").

[366] The estimate is reported in Priscilla M. Regan, *Legislating Privacy* 233 (1995). *See also* Robert J. Posch, Jr., *Keep the Privacy Debate in Context*, Direct Marketing, May 1, 1997 (quoting DMA President H. Robert Wientzen that "Mechanically and cost-wise, [opt in makes it] much too difficult to achieve the penetration that you need to make e-mail direct marketing a viable concept.").

[367] *Panel One: Information Issues: Intellectual Property, Privacy, Integrity, Interoperability, and the Economics of Information*, 48 Fed. Com. L. J. 5, 41 (1995) (remarks of Ellen M. Kirsh, Vice-President, General Counsel, and Secretary of America OnLine, Inc.).

[368] FTC, Public Workshop on Consumer Information Privacy, Session Two: Consumer OnLine Privacy, at 109-10 (June 12, 1997) (available on the web at <http://www.ftc.gov/bcp/privacy/wkshp97/index.html> (last checked Aug. 21, 1998) (remarks of Rosalind Resnick, President, Net Creations, Inc.). The company's website can

1,000 percent in twelve months.[369] Other companies offer consumers incentives to opt-in to internet solicitations.[370] Equifax established "Buyer's Market," an opt-in service under which a million consumers filled out a list of the kinds of mail they wished to receive--or didn't wish to receive.[371] The company eventually charged a modest fee for participating, but subscribers also received discounts on products.[372] In the nineteen-eighties, National Consumer Research charged consumers $199 to have their names and purchasing habits included in a database. The information was provided to direct marketers which then provided discounts to those listed in the database. About 10,000 consumers are said to have signed up.[373]

Our marketing system is premised on the assumption that consumers are persuadable. Enormous sums are spent to convince consumers of the merits of particular purchases--enough to finance commercial television and radio, underwrite a significant portion of the newspaper and magazine businesses, and, of course, to pay for the direct mail and telemarketing industries, among others. Our economy is a positive-option system, not a negative-option system, in which consumers make purchasing decisions--often, at least so it appears--at the suggestion of marketers. It seems ironic that marketers believe in what they do on behalf of others, but doubt that they can be effective on their own behalf.

---

be found at <http://www.postmasterdirect.com.>

[369] Letter from Rosalind Resnick, President, Net Creations, Inc, to FTC (May 10, 1997), available at <http://www.ftc.gov/bcp/privacy/wkshp97/comments2/ftcoptin.html> (last checked Aug. 21, 1998).

[370] For example, BonusMail (available at <http://www.bonusmail.com> (last checked Oct. 14, 1998)) provides consumers with frequent flyer miles and other rewards for receiving e-mail while CyberGold (available at <http://www.cybergold.com> (last checked Oct. 14, 1998)) pays consumers to read ads. *See also* Teresa Riordan, *Patents*, N.Y. Times, Feb 1, 1999 at C2.

[371] Erik Larson, *The Naked Consumer* 101 (1992).

[372] Mark D. Uehling, *Database Marketing: Here Comes the Perfect Mailing List*, American Demographics, Aug. 1991 at 10 ($15 fee); *What Price Privacy?* Consumer Reports 356, 360 (May 1991). S*ee also* Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 Computer & High Tech. L. J. 431, 462 (1993). In 1992 Equifax spun the division--now called Buyer's Choice Media--off as an independent company. Judith Waldrop, *The Business of Privacy*, American Demographics, Oct. 1994, at 46 (quoting Keith Wardell of Buyer's Choice Media).

[373] Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Public Pol. & Marketing 149, 161

Even in an opt-in system, businesses would still have significant advantages in convincing consumers to opt in. While companies would have a tremendous incentive to persuade consumers to opt in, no organization would have a comparable reason to discourage consumers from opting in. More than twelve million people are employed in selling and advertising.[374] Only about 1,000 people work for the two largest consumer information organizations, Consumers Union (publishers of Consumer Reports) and the American Association of Retired Persons.[375] Hence, marketers, with their greater incentive and resources would be able to make a powerful case that consumers should opt in while the opposing viewpoint would probably be much less forcefully expressed. Undoubtedly some consumers would not opt in. But it is also likely that many others would.

Predictions that significant privacy legislation would be costly are undermined by comparing predictions of the costs made in the past by opponents of consumer legislation, with the actual costs of such legislation once it was enacted. For example, before Congress passed an amendment to the Equal Credit Opportunity Act ("ECOA") to require creditors to disclose the reasons for an adverse decision on a credit application, [376] it received testimony in 1975 from the National Retail Merchants Association that

> Sears Roebuck and Company stated that its annual estimated cost for such compliance would be approximately $5 per letter. * * * Even if all creditors could operate as efficiently as Sears, the aggregate annual cost of this requirement could easily amount to hundreds of millions of dollars. [377]

(1991). Consumers also received bounties for signing up new members.

[374] E. Scott Maynes, *Consumer Problems in Market Economies* in *Encyclopedia of the Consumer Movement* 158 (Stephen Brobeck, ed. 1997).

[375] E. Scott Maynes, *Consumer Problems in Market Economies* in *Encyclopedia of the Consumer Movement* 158 (Stephen Brobeck, ed. 1997).

[376] The provision appears at 15 U.S.C. § 1691(d).

[377] U.S. Sen., Com. on Banking, Housing, and Urban Affairs, Subcom. on Consumer Affairs, *Hearings on S. 483, S. 1900, S. 1927, S. 1961, and H.R. 6516* at 399 (1975) (testimony of National Retail Merchants Association).

After the provision was enacted, a Federal Reserve Board survey found that the average cost per Sears account of providing the reasons for denying credit was only 59 cents, far less than the original estimate of $5 per letter.[378] Similarly, when Equifax asked executives in 1990 whether ECOA had significantly increased business costs, 66% of credit grantor executives and 59% of executives at banks and thrifts said it had not. Only 22% and 35% of the executives at the credit grantors, and banks and thrifts, respectively, said it had.[379] And they were dealing with all the provisions of a statute that bars lenders from considering certain criteria in making lending decisions, asking certain questions, provides for punitive damages, and has led to other changes in lending practices.[380] Proposals to change consumer law to aid consumers frequently draw objections based on cost estimates that later prove to be wildly inflated.[381]

D. A Hybrid Proposal

The National Telecommunications and Information Administration (NTIA) of the Department of Commerce has proposed a hybrid opt-out, opt-in system. Under the NTIA approach, companies could not use "sensitive" information unless the consumer opted in, but could use non-sensitive information as long as the company notified the consumer that the

---

[378] Board of Governors of the Federal Reserve System, *Exercise of Consumer Rights Under the Equal Credit Opportunity and Fair Credit Billing Acts*, 64 Fed. Res. Bull. 363, 365 (1978). The 59 cents figure appears to have been based on information provided by Sears in response to a Federal Reserve inquiry.

[379] *1990 Equifax Privacy Report*, *supra*, note ___ at 92.

[380] *See, e.g.,* 15 U.S.C. § 701(a)(1) (barring lenders from discriminating on the basis of race, color, religion, national origin, sex, or marital status); § 706 (punitive damages of up to $10,000 for individuals and up to the lesser of $500,00 or 1% of creditor's net worth for class actions); 12 C.F.R. § 202.5(c) (implementing regulation forbidding asking of certain questions). On ECOA, *see generally* Dee Pridgen, *Consumer Credit and the Law*, chap. 3 (1996); Michael M. Greenfield, *Consumer Law* 337-94 (1995).

[381] *See, e.g.* Daniel D. Cutler, *The Continuing Struggle for Automotive Safety*, 15 Seton Hall Legis. J. 453, 463 n.65 (1991) (car manufacturers estimated airbags would cost consumers $1,100); Jeff Sovern, *Good Will Adjustment Games: An Economic and Legal Analysis of Secret Warranty Regulation*, 60 Mo. L. Rev. 323, 338 (1995) ("Proposals designed to aid consumers often elicit predictions of . . . setbacks for consumers, and the predictions have sometimes proved fanciful. Thus, some forecast that sellers would stop warranting goods if Congress passed the Magnuson-Moss Warranty Act, and obviously sellers still furnish warranties.") (footnotes omitted); Robert J. Banta, *Negotiability in Consumer Sales--the Need for Further Study*, 53 Neb. L. Rev. 195, 196-97 (1974) ("Many banking and financial institutions argue that if they were subject to consumer defenses, consumer credit might vanish or become so expensive as to be prohibitive.").

consumer could prevent the use of the non-sensitive information by sending in a form or making a telephone call by a certain date. [382] NTIA acknowledges that the definition of sensitive information "is not clear-cut" and gives as examples health care information, political persuasion, sexual matters and orientation, personal finances, and social security numbers. [383]

NTIA points out several advantages to such a system. First, to the extent that the defaults reflect consumer preferences, it will minimize transaction costs: if consumers generally wish to prevent the sale of sensitive information but do not object to the sale of non-sensitive data, they can simply do nothing; their preferences will be accommodated by the default settings. [384] And second, it gives consumers greater control over sensitive information.

But the NTIA system may be flawed. It requires someone to define what information is sensitive and what is not. That the definition is not instantly obvious is suggested by NTIA's failure to create its own definition. To the extent that the definitions do not conform to an individual's own preferences, that individual will have to incur transaction costs--or live with a system that does not reflect the consumer's preferences--and so the chief rationale for the NTIA system will disappear. One thing that emerges from the available survey data is that consumers are in fact split about many privacy issues. As Erik Larson has written, "What is private to one individual may not be private to his neighbor; what is considered private today may not be considered private tomorrow."[385] Indeed, when the Federal Reserve System invited comments

---

[382] U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 25 (1995). *See also* Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*,1996 U. Chi. L. Forum 77, 137 (making similar proposal).

[383] U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 25 (1995).

[384] U.S. Dept. of Commerce, National Telecommunications and Information Admin., *Privacy and the NII: Safeguarding Telecommunications Related Personal Information* 26 (1995).

[385] Erik Larson, *The Naked Consumer* 10 (1992).

on what constitutes sensitive information, it found "widely varying answers." [386] Accordingly, it may be that so many consumers would not be satisfied with the NTIA defaults that the system would not produce any savings in transaction costs. The NTIA system may in fact conform to the views of enough consumers so that it does produce savings in transactions costs--but it is not demonstrable on the basis of the evidence currently available that that is so. It may be that a default that prevents any trade in personal information absent permission from the affected consumer is consistent with the views of more consumers and thus would incur lower transaction costs from consumers shifting their defaults.

A better solution than the NTIA approach would focus not on the nature of the information but on consumer preferences. When a significant proportion of consumers want to prevent the sale of their information, an opt-in system could be used. On the other hand, when a significant proportion of consumers do not object to the reporting of their information, an opt-out system could be used. That maximizes the number of consumers whose defaults would correspond to their preferences, and so would not have to incur transaction costs in contracting around the defaults.

What percentage of consumers is large enough to warrant switching from an opt-in default to an opt-out default? If the problems with strategic behavior costs and the like did not exist, a simple majority might be the trigger. But the incentive and ability to inflate transaction costs changes the calculus. Ideally, the percentage should be set at the point where the cost of opting in, plus losses from consumers who prefer receiving solicitations not opting in, equal or exceed the losses from strategic behavior costs which would occur in an opt-out system, plus the

[386] Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 14 (1997). After listing various items that some commenters regard as sensitive and others did not, the report observes "A determination of what is sensitive is largely subjective. . . . information that one person considers not to be sensitive, because it reveals little, may be sensitive to another person. Thus, while a current telephone number may not be considered sensitive, or even private, to people who have their numbers listed in the local telephone directory, it may be highly sensitive for

cost of consumers opting out. But because it is impossible to determine what those figures are, the best approach may simply be to require a large percentage of consumers who prefer that their information be used --perhaps as high as 75% or even higher--before the rule switches from "information cannot be used unless the consumer affirmatively permits it" to "information can be used unless the consumer acts to prevent it."

For example, comparatively few consumers mind the use of their personal information to determine if they should be granted credit for which they have applied. [387] Using an opt-out system with credit applications makes sense because it permits most consumers to do nothing and still attain their desires. The few consumers who do not want their information used for that purpose would still have the capacity to opt out. An opt-in system serves little purpose in such circumstances because it forces most consumers to incur transaction costs while benefiting few consumers.[388]

VI. Conclusion

I have argued in this Article that under the present regime, in which the trade in consumer

---

someone who has an unlisted number." *Id*. at 15.

[387] See *supra* note ___ and accompanying text. This preference is consistent with economic theory. *See* George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. Leg. Studies 623, 625-26 (1980):

> [I]f all credit-history information, for example, were "owned" by the debtor, and there were not a special difficulty in enforcing this ownership because of the public good character of information, this inherent partnership in producing information would create no special problems. I would have an established credit record with the merchant with whom I customarily dealt, and be charged for credit according to the cost of dealing with me (including the cost of learning my payment habits). Another merchant, to whom I denied access to my regular merchant's information, would charge for credit appropriately to his ignorance of my credit worthiness, so in general it would pay me to ask the regular merchant to supply the credit record to others. This would be true even if I were a poor credit risk: the new merchant would extend credit only at high charges to those who refused to reveal their previous records. In the long run, in a sequence of many repetitive transactions, even a poor credit risk can do no better than to deal with informed creditors. . . . The economy of the multiple use of the same information should be accommodated no matter how the ownership of the information is assigned. The failure of contracts to emerge which specify that the creditor may not sell the consumer credit information is in the interest of debtors, for whom credit would otherwise be more expensive.

[388] *Cf.* Ian Ayres & F. Clayton Miller, "*I'll Sell it to You at Cost:" Legal Methods to Promote Retail Markup Disclosure*, 84 Nw. U. L. Rev. 1047, 1076 (1990) ("Requiring . . . disclosure when the costs of communicating are higher than the value of the information to consumers would force retailers to provide a service

information is largely unregulated, [389] businesses have both an incentive and the ability to inflate consumer transaction costs in preventing the use of personal information. As a result, more consumer information is available and more solicitations are made than would be the case if

---

whose value is less than its costs.").

[389] Most uses of consumer information are unregulated. A few exceptions exist, however. For example, when Congress amended the Fair Credit Reporting Act in 1996, 15 U.S.C. § 1681 et seq., it created an opt-out system for pre-screening. The statute forbids consumer reporting agencies to use information about consumers who object to the pre-screening process. 15 U.S.C. § 1681b(e). *See also* Mass. Gen. Laws tit. 15, § 51A. The federal statute also requires consumer reporting agencies to establish a notification system for consumers to opt-out. 15 U.S.C. § 1681b(e)(5). Consumer reporting agencies must maintain toll-free telephone numbers for consumers to express their preferences and advertise the availability of the opt-out system. Those who obtain the names and addresses of consumers through pre-screening must notify the consumers whom they solicit of the consumer's right to opt-out. 15 U.S.C. § 1681m(d)(1)(D), (E). It remains to be seen how effective this particular opt-out system will be. Similarly, consumers may obtain from the Postal Service an order barring specified people from mailing them materials which are "erotically arousing or sexually provocative." 39 U.S.C. § 3008. The Postal Service order must also forbid the mailer from selling the consumer's name to others. Telemarketers are required to maintain a list of consumers who have told the telemarketer that they object to receiving marketing calls, and to refrain from calling consumers on the list. 47 C.F.R. § 64.1200(e).

Some states have also created opt-out systems. California now requires credit card issuers that sell consumer information to notify the cardholder before the sale and offer the cardholder the opportunity to opt-out. Cal. Civ. Code § 1748.3(b). A cardissuer must either provide cardholders with a preprinted opt-out form or maintain a toll-free telephone number for that purpose. Cal Civ. Code § 1748.3(b). The statute does not apply to information furnished to credit reporting agencies by the cardissuer. Cal. Civ. Code § 1748.3(e)(2). Virginia also has an opt-out statute. The statute bars merchants engaged in the sale of goods from a "fixed retail location in Virginia" from selling "to any third person information which concerns the purchaser and which is gathered in connection with the sale, rental or exchange of tangible personal property to the purchaser at the merchant's place of business" unless the merchant gives notice to the consumer. Va. Code § 59.1-442. The merchant may give that notice "by the posting of a sign or any other reasonable method." Va. Code § 59.1-442. Merchants who give the requisite notice may still not sell consumer information about any consumer who objects to the sale. The statute has several limits. First, it does not apply to services. Second, it is limited to merchants with a retail outlet in Virginia. Third, it is not clear whether the statute extends to mail-order sales or sales made over the telephone--are such sales made to the purchaser at the merchant's place of business? In addition Quebec has enacted an opt-out law for mailing lists. Act Respecting the Protection of Personal Information in the Private Sector, S.Q., ch. 17, § 13 (1993). The president of the Commission charged with enforcing the statute reported a year after its adoption that "There has been no catastrophe in Quebec. It's business as usual. The implementation of this important piece of legislation is running smoothly." Remarks of Paul-Andre Comeau, president of the Commission d'Access a l" Information, quoted in Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* 187 (1997). *See also* Paul-Andre Comeau & Andre Ouimet, *Freedom of Information and Privacy: Quebec's Innovative Role in North America*, 80 Iowa L. Rev. 651, 668 (1995) ("The legislation is considered viable in that enterprises can 'live with it.' The decisions taken spontaneously by some enterprises outside Quebec provide indirect proof of this as they use the same consent form in their transactions with their customers or members in the rest of Canada as well as Quebec.").

Two states have passed statutes regulating unsolicited commercial e-mail. Nevada requires that unsolicited e-mail advertisements inform the recipient how to notify the sender that the recipient declines to receive further e-mail advertisements from the sender. Nev. Rev. Stat. tit. 3, § 41.730. Washington bars the knowing transmission of unsolicited commercial e-mail to Washington residents if the message uses a third party's internet domain name without permission; misrepresents any other information in identifying the origin or transmission path of the message; or contains false or misleading information on the subject line. *See* 1998 Wa. ch. 149. Oddly, the law does not require senders to inform consumers how to remove themselves from lists or even that senders remove consumers from lists upon demand. The Washington State Attorney General's Office has sued at least one spammer for violating the statute. *See* Tina Kelley, *Lawsuit Against a Spammer is Filed Under a Oregon Law*, [sic] N. Y. Times, Oct. 29, 1998, at G3.

unnecessary transaction costs were eliminated. While some are attempting to self-regulate, the failure of past attempts at self-regulation and the atomistic nature of the consumer information industry justifies pessimism about whether such attempts will succeed. Accordingly, government intervention seems desirable.

That intervention should logically take one of two forms: either government should preserve the existing system--in which consumer information may be used and sold unless the consumer objects--but should insure that consumers are adequately informed about the uses of their information and given a chance to opt out of that use--or government should impose an opt-in system in which consumer information may not be used or sold unless the consumer to whom the information pertains affirmatively consents to the use. An opt-in system eliminates the incentive businesses have to inflate transaction costs and thus seems more likely to produce an efficient outcome.