

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

Jeff Sovern*

Abstract: Businesses routinely buy and sell personal information about consumers. Many consumers find this objectionable, but relatively few of them opt out of that trade. This Article argues that businesses have both the incentive and the ability to increase consumers' transaction costs in protecting their privacy and that some marketers do in fact inflate those costs. Faced with this and other constraints, many consumers ultimately decide not to protect their privacy. This Article proposes several ways by which consumers' transaction costs can be reduced or eliminated.

A few years ago one of my students told me he had a copy of my driving record.¹ During a later class he asked if I

* 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.

1. Driving records in New York are available to the public. See N.Y. Veh. & Traf. Law § 508.3 (McKinney 1996) ("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, sellers of eyeglasses use them to identify consumers who require corrective lenses. 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 B5. Some states make a significant amount of money from selling drivers' information. See Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law* 150 (1996); *What's in a Name? Big Bucks*, Albany Times Union, May 8, 1996, at A14 (reporting that state sold list of drivers for \$1.4 million). However, there are states that either do not release the data or use an opt-out procedure under which drivers may prevent disclosure of their information. See Schwartz & Reidenberg, *supra* at 150.

In 1994, Congress enacted the Driver's Privacy Protection Act, Pub. L. No. 103-322, 108 Stat. 2102 (codified at 18 U.S.C. §§ 2721-2725 (1994)), to restrict access to information in state motor vehicle records. The Act lists, in 12 subsections, permissible uses of drivers' personal information. See 18 U.S.C. § 2721(b)(1) - (10), (13), (14) (1994). 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 has given consumers the opportunity to prevent the disclosure. 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 in *infra* note 22. 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), *cert. granted*, 119 S. Ct. 1753 (1999). *But see* *Travis v. Reno*, 163 F.3d 1000 (7th Cir. 1998)

wanted a list of my neighbors.² On other occasions he correctly told me the name of one of my brothers and the lienholder on my co-op apartment. Once he gave me a bullet.³ Though the story is a little frightening, this was hardly an obsession for him; he was just having fun, sandwiched between the demands of class and work. 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.

The information available on consumers is striking. For example, you can buy lists of people who have bought skimpy swimwear; college students sorted by major, class year, and tuition payment; millionaires and their neighbors; people who have lost loved ones; men who have bought fashion underwear; women who have bought wigs; callers to a 900-number national dating service; rocket scientists; children who have subscribed to magazines or have sent in rebate forms included with toys; people who have had their urine tested; medical malpractice plaintiffs; workers' compensation claimants; people who have been arrested; 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.⁴ There are lists

(upholding statute); *Oklahoma v. United States*, 161 F.3d 1266 (10th Cir. 1998) (same); *Pryor v. Reno*, 998 F. Supp. 1317 (M.D. Ala. 1998) (same). For an argument that government may not 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).

2. This information is available in a computer database. The information is useful to creditors searching for debtors who have moved. For example, the database allows the creditor to identify the debtor's former neighbors, from whom the creditor might obtain the debtor's whereabouts. See William M. Bulkeley, *Bill Collectors Master Automated Arm-Twisting*, Wall St. J., Sept. 10, 1990, at B1.

3. 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.

4. See Oscar H. Gandy, Jr., *The Panoptic Sort* 91 (1993); Erik Larson, *The Naked Consumer* 63–64, 93 (1992); National Telecomm. & Info. Admin., U.S. Dep't of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, app. at A-3 (1995)

based on⁵ ethnicity, political opinions, and sexual orientation.⁵

The media is filled with horror stories about the use of personal information. Stories on the availability of information most people consider confidential routinely appear.⁶ A television reporter—without any proof of identification—obtained, overnight, a list of 5000 families, including addresses and the names of children, for \$277. The reporter used the name of Richard Allen Davis, who was on trial for kidnapping and killing a twelve-year-old at the time.⁷

[hereinafter *Privacy and the NII*]; Schwartz & Reidenberg, *Data Privacy Law*, *supra* note 1, at 322; H. Jeff Smith, *Managing Privacy* 100 (1994); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497, 519–20, 523 (1995); *Merchants of Data: Are They Telling on You?*, 56 Consumer Rep. 356 (1991); Robert O'Harrow, Jr., *For Sale on the Web: Your Financial Secrets; Bank Accounts Vulnerable to Data Brokers*, Wash. Post, June 11, 1998, at A1; Larry Tye, *List-Makers Draw a Bead on Many*, Boston Globe, Sept. 6, 1993, at 1; *Your Health Files: How Insurers Check*, 56 Consumer Rep. 357 (1991).

5. See *Privacy and the NII*, *supra* note 4, app. at A-3 (“[L]ist 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.’ ”); Reidenberg, *supra* note 4, at 519–20, 523; Susan Headden, *The Junk Mail Deluge*, U.S. News & World Rep., Dec. 8, 1997, at 43; Martin J. Smith, *Ever Wonder Why You Get All That Unsolicited Junk Mail?*, Ariz. Republic, Dec. 5, 1993, at A1 (noting that Hispanic New Movers File containing 1.85 million names is available for \$70 per thousand names); Tye, *supra* note 4, at 1 (listing those with Italian, Japanese, and 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 (listing 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).

6. See, e.g., Larson, *supra* note 4, at 58 (“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.”); Margot Williams & Robert O'Harrow, Jr., *Online Searches Fill in Many Holes*, Wash. Post, Mar. 8, 1998, at A19 (reporting on free web service that 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).

7. See Evan Hendricks, *Metromail Stung Again*, Privacy Times, May 17, 1996, at 4; see also Ann Reilly Dowd, *Protect Your Privacy*, Money, Aug. 1997, at 112 (“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.”).

Some reports are so overwhelming they are mind numbing. One company claims to have identified a market segment for every household in the United States,⁸ while another advertises that its database lists every registered voter, as well as his or her telephone number, address, and ethnic surname identification.⁹ A business executive estimates that on a normal day the average American's personal information moves from one computer to another five times.¹⁰ The typical person is said to appear in anywhere from 25 to 100 databases.¹¹ A person sued a marketing company, only to discover that the company's dossier on her was twenty-five pages long.¹² The computer library of an information service few have even heard of, Acxiom Corporation, reportedly has 350 trillion characters of consumer data on more than 195 million Americans.¹³ Services peddle bank account balances,¹⁴ unlisted telephone numbers, and salary figures.¹⁵ In Joel Reidenberg's words, the "private sector has precisely the

8. See Gandy, *supra* note 4, at 92. The U.S. 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 consisting of 133 million individuals. See *Privacy and the NII*, *supra* note 4, app. at A-2 n.10.

9. See Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. Chi. Legal F. 77, 96 (1996) (citing Aristotle Industries' advertisement in Campaigns & Elections, Feb. 1995, at 83).

10. See 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).

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

12. See Nina Bernstein, *Personal Files Via Computer Offer Money and Pose Threat*, N.Y. Times, June 12, 1997, at 1 ("[The 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 deodorizers, sleeping aids and hemorrhoid remedies.").

13. See Michael Fraase, *Information Eclipse, Privacy and Access in America* 155 (1999); Robert O'Harrow, Jr., *Data Firms Getting Too Personal?*, Wash. Post, Mar. 8, 1998, at A1.

14. See Robert Douglas et al., *How Your Financial Privacy Is Threatened*, Consumers' Res. Mag., Dec. 1998, at 10; O'Harrow, *supra* note 4, at A1.

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

type of dossiers that the public has long feared government would abuse.”¹⁶

Even the lists of lists are voluminous. A list directory describes more than 10,000 lists which can be purchased.¹⁷ The Direct Marketing Association, a trade association, estimates that more than 15,000 consumer mailing lists exist, containing some two billion names (including duplicates).¹⁸ More than 1000 commercial services are said to broker lists.¹⁹

Not only is more personal information available than ever before, but it is becoming easier and less expensive to obtain access to it.²⁰ Internet sites, and even Westlaw, have databases designed to locate individuals and to report on their transactions—including their bankruptcy records, lawsuits, liens, real property refinancings, and transfers—and the location of their assets.²¹ Other Internet

16. Reidenberg, *supra* note 4, at 536.

17. Direct Mail List Rates and Data, compiled by Standard Rate and Data Service, is referred to in Jill Smolowe, *Read This!!!!!!*, Time, Nov. 26, 1990, at 62, 66; see also Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 Fed. Comm. L.J. 195, 202 n.29 (1992). One company alone reportedly maintained 1600 databases containing more than 3.5 billion public records. See Rajiv Chandrasekaran, *Doors Fling Open to Public Records*, Wash. Post, Mar. 8, 1998, at A1.

18. See Paula Crawford Squires, *Transactions Go into a Database; Businesses Compile Dossiers on Customers*, Richmond Times Dispatch, July 28, 1996, at A-12.

19. See *Privacy and the NII*, *supra* note 4, app. at A-2.

20. See, e.g., *id.* (“[B]ecause 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.”); Bernstein, *supra* note 15, at A1 (describing service that provides Social Security number, date of birth, and telephone number in less than three minutes and for about \$1.50; “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 Pers. Fin. 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.]”); Evan Hendricks, *CDB’s Cut-Rate Look-Up Service*, Privacy Times, Feb. 20, 1998, at 8 (reporting cost of look-up service, which provides subject’s name, aliases, current and previous 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).

21. 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

sites list driver's license and motor vehicle information, and verify Social Security numbers.²² The number of web sites selling personal information is estimated at several thousand.²³ Prices for many services are now at the point where information that formerly could be afforded only by businesses is now accessible to individuals.²⁴

Access to some information—such as credit reports—is regulated, although that may be of small comfort to celebrities who have discovered their credit reports in the hands of strangers.²⁵ Still, the use of other data, including much of those referred to in the preceding paragraphs, are generally not subject to any legal restraint. For example, a

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 that can be used to find people is Database America, at <<http://www.databaseamerica.com>>. Another Internet site which provides information on assets, lawsuits, liens, bankruptcy records, refinancings, and other information is KnowX, at <<http://www.knowx.com>>. Lexis-Nexis also has two services designed to locate people: P-Trak and P-Find. For a discussion of what these services can do, see FTC, *Public Workshop on Consumer Information Privacy Session One: Database Study* (June 10, 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/volume1.pdf>> [hereinafter FTC, *Session One: Database Study*] (remarks of Karen Welch, Strategic Account Consultant, Lexis-Nexis).

22. See American Info. Network Inc., *The Internet Department of Motor Vehicles* (visited Oct. 6, 1999) <<http://www.ameri.com/dmv.htm>> (charging fee for access to driver's license and motor vehicle information); Informus Corp. (visited Oct. 6, 1999) <<http://www.informus.com>> (providing access to Social Security numbers, credit reports, and criminal records for fees under \$25); Glen Roberts, *The Stalker's Home Page* (visited Oct. 6, 1999) <<http://www.glr.com/stalk.html>> (containing links to other web sites that verify Social Security numbers and provide other personal information); Search First Info. Serv. (visited Oct. 6, 1999) <<http://www.searchfirst.com>> (providing access to driver's license information, Social Security number verification, credit report, and criminal records, for various fees under \$50).

23. See O'Harrow, *supra* note 13, at A1.

24. See *Privacy and the NII*, *supra* note 4, app. at A-7 n.30. Some services provide information to anyone who pays a fee. See FTC, *Session One: Database Study*, *supra* note 21, at 45–46 (describing subscription-free services available on Internet).

25. See, e.g., Rothfeder, *supra* note 10, at 17–21 (reporting on Vice-President Dan Quayle's Sears and Brooks Brothers accounts, Social Security number, and credit card number); Ellen R. Foxman & Paula Kilcoyne, *Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues*, 12 J. Pub. Pol'y & Marketing 106, 111 (1993) (describing how authors obtained CBS News Anchorperson Dan Rather's credit report, charge card data, mortgage information, location of residence, shopping information, and dining information); cf. *Privacy and the NII*, *supra* note 4, at 4 (reporting journalists' discovery of financial, legal, marital, and residential histories of movie producer George Lucas and White House Chief of Staff Leon Panetta). In 1997, amendments to the Fair Credit Reporting Act went into effect, which may offer more protection for credit reports. See 15 U.S.C.A. § 1681 (West Supp. 1999).

service gave out the home address of Kurt Schmoke (Mayor of Baltimore), as well as the property's purchase price, mortgage amount, and taxes.²⁶ 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."²⁷

Businesses use the information available to them for a variety of purposes, the best known of which is to solicit sales. Each year Americans reportedly receive sixty-three billion pieces of junk mail, as well as billions of telemarketing calls.²⁸ But the information is also used for other purposes. 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 low-calorie foods such as yogurt and reduced-fat breads. The company marketed the list to sellers of fitness equipment, vitamins, and clothing. It also offered a list of "fancy food buyers"—consumers who bought refrigerated pastas or frozen yogurt—to travel magazines and sellers of "high-ticket gifts."²⁹

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.³⁰ For

26. See Larson, *supra* note 4, at 61.

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

28. See Rothfeder, *supra* note 10, at 90.

29. Miller, *supra* note 1, at B1; see also Larson, *supra* note 4, at 134–36 (describing similar marketing techniques).

30. See Roger Clarke, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*, 4 J.L. & Info. Sci. 403 (1993). For examples, see Daniel Mendel-Black & Evelyn Richards, *Peering into Private Lives: Computer Lists Now Profile Consumers by Their Personal Habits*, Wash. Post, Jan. 20, 1991, at H1:

Vacuumed into huge databases around the country is information about how many times you went out to eat last month, about whether your 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 . . . [C]lashing 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?, 56 Consumer Rep. 356 (1991), also states:

example, one company identifies hobbies, reading habits, jobs, vacation preferences, and pets, and makes predictions about future purchases.³¹

Other notable stories abound. One company acquired names of consumers and their prescription information from pharmacies and then sent those consumers reminders to refill their prescriptions or solicitations to switch to competing drugs, communications which were partly financed by drug manufacturers.³² Another company maintains a "birthday bank" containing 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 who might splurge as a result.³³ The same company also maintains records on consumer heights and weights, information of interest to clothing sellers.³⁴

Even the manner in which databases are created has raised questions. Richard 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*

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 database 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).

31. See O'Harrow, *supra* note 13, at A1.

32. See Evan Hendricks, *Class-Action Suit Targets CVS over Use of Prescription Data*, *Privacy Times*, Apr. 3, 1998, at 1, 2; see also Center for Pub. Integrity, *Nothing Sacred* 27 (1998) (describing woman who, after visiting doctor for routine tests, received letter from "pharmaceutical company that had obtained access to her medical data and wanted her to try its new cholesterol medication"); Evan Hendricks, *Rising Traffic in Prescription Info Causes Backlash in D.C.*, *Privacy Times*, Feb. 20, 1998, at 1, 2 [hereinafter Hendricks, *Rising Traffic in Prescription Info*] (noting that efforts to market antidepressants and schizophrenia drugs to mental health patients is "particularly controversial because of the greater potential for manipulation"); Sheryl G. Stolberg, *The Numbering of America: Medical I.D.'s and Privacy (or What's Left of It)*, *N.Y. Times*, July 26, 1998, § 4 at 3.

33. See Rothfeder, *supra* note 10, at 91–92.

34. See *id.* at 92.

information.”³⁵ 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 TVs. The commercial then played tones that dialed an 800 number. A mechanism automatically recorded the telephone number of phones from which calls to the 800 number were placed.³⁶ The manufacturer then obtained the names and addresses that matched the telephone numbers, creating a mailing list.

Adults are hardly immune from such tricks. In 1993, the manufacturer of a product for incontinent women established a toll-free number for people who wanted free samples. It then offered for sale a list of the 4.4 million people who responded.³⁷ In another example, a woman began receiving solicitations directed toward lesbians after

35. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381, 2402 (1996) (emphasis in original); cf. Mary J. Culnan & Sandra J. Milberg, *The Second Exchange: Managing Customer Information in Marketing Relationships* (visited May 19, 1999) <www.msb.edu/faculty/culnanm/home.html> (“[T]he first exchange of goods or services . . . is accompanied by what we . . . call a ‘second exchange’ of personal information for a variety of customized tangible or intangible benefits.”).

36. See Gary T. Marx, *Privacy & Technology*, *Whole Earth Rev.*, Winter 1991, at 90, 91; see also Foxman & Kilcoyne, *supra* note 25, at 110 (describing technology that allows subscribers to call toll-free numbers to obtain lists of callers’ numbers); Mendel-Black & Richards, *supra* note 30 (“[D]ialing an 800 number can put your name and address on a list.”).

37. See Kevin DeMarrais, *Big Brother Is Watching Your Database*, *The Record*, Apr. 30, 1995, at A1; see also Rothfeder, *supra* note 10, at 92–93 (describing 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, *Companies Exploiting Internet’s Ability to Track Consumer Habits*, *Privacy Times*, July 3, 1995, at 3, 4 (reporting on company that 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); Hendricks, *Rising Traffic in Prescription Info*, *supra* note 32, at 1, 3 (reporting on drug companies said to capture phone numbers from consumers calling toll-free numbers for various medications). 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; consequently, Western Union must comply with the Fair Debt Collection Practices Act, 15 U.S.C. § 1692a(2) (1994). See *Romine v. Diversified Collection Serv., Inc.*, 155 F.3d 1142 (9th Cir. 1998).

spending one night at a lodge which, she later learned, catered primarily to lesbians. The lodge had sold her name to a lesbian-mailing-list compiler.³⁸

Similarly, the Federal Trade Commission has determined that businesses operating web sites collect a great deal of information from consumers, including children, often without disclosing to consumers how the information will be used.³⁹ Ninety-two percent of the web sites in one sample collected personal information such as Social Security number, gender, and age.⁴⁰ Nearly ninety percent of the web sites directed at children also collect personal information.⁴¹ To gather information from children, web sites use fictional characters to pose questions, have children sign guest books, solicit information to create home pages for children, invite children to join electronic chat and pen-pal programs, require children to register with the site, or offer prizes and other incentives for providing information.⁴² 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.⁴³

38. See Tye, *supra* note 4, at 1.

39. See FTC, *Privacy Online: A Report to Congress* 22, 27 (1998) [hereinafter FTC, *Privacy Online*]. On the other hand, a more recent study found that nearly two-thirds of the sites in its sample contained at least one privacy disclosure. See Mary J. Culnan, *Georgetown Internet Privacy Policy Survey* 7 (1999).

40. See FTC, *Privacy Online*, *supra* note 39, at 23, 25. The FTC took a number of different samples of web sites, the largest of which it labeled the Comprehensive Sample. Other samples include: Retail Sample, Financial Sample, Children's Sample, and Most Popular Sample. Unless otherwise indicated, information reported in this Article relates solely to the Comprehensive Sample.

41. See *id.* at 31.

42. See *id.* at 32, 33; see also Shelley Pasnik & Mary Ellen R. Fise, *Children's Privacy and the GII*, in *Privacy and Self-Regulation in the Information Age* (visited Oct. 6, 1999) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>>.

43. See FTC, *Privacy Online*, *supra* note 39, at 36–37. After FTC issued the report, Congress enacted the Children's Online Privacy Protection Act, Pub. L. 105-277, 112 Stat. 2681 (1998). That statute regulates the collection of information from children in online transactions and requires parental approval for the collection and retention of certain information. The FTC has since proposed a rule to implement the statute. See 64 Fed. Reg. 22,750 (1999).

Stories like these—involving conflicting desires for privacy and for information that may be of some value—have become commonplace.⁴⁴ Privacy, of course, means different things to different people.⁴⁵ This Article concerns what some call “informational privacy”⁴⁶ and others call confidentiality or data protection.⁴⁷ These are rights an individual has or should have to prevent third parties from obtaining, using, and selling private information. This Article also addresses the rights of third parties to use that information without the knowledge or consent of the individual to whom the information pertains.

Laws regulating personal information—especially information contained in 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 fundamental principles and policies.⁴⁸ Thus,

44. As Arthur Miller puts 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).

45. See, e.g., Alan F. Westin et al., *The Equifax Report on Consumers in the Information Age* xviii (1990) [hereinafter *1990 Equifax Report*] (“[P]rivacy is the claim of individuals to decide what information about themselves will be communicated to others.”); Charles Fried, *Privacy: Economics and Ethics—A Comment on Posner*, 12 Ga. L. Rev. 423, 423 (1978) (“[P]rivacy is to be defined as the control of information about oneself.”); Charles Fried, *Privacy*, 77 Yale. L.J. 475, 493 (1968); 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) (“[P]rivacy 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 Denv. L.J. 449, 450 (1983) (defining privacy as “the unitary concept of separation of self from society”); see also Fred H. Cate, *Privacy in the Information Age* 19–31 (1997) (canvassing definitions).

46. See, e.g., Jacob Sullum, *Secrets for Sale*, Reason, Apr. 1992, at 29 (“[T]he amorphous concept of informational privacy, variously described as a right, a concern, an interest, and a preference.”).

47. See, e.g., Cathy Goodwin, *Privacy: Recognition of a Consumer Right*, 10 J. Pub. Pol’y & Marketing 149, 149 (1991).

48. Among privacy statutes regulating commerce (as distinct from statutes governing government-held data) are the Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (1994) (governing bank records), the Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681t (1994) (governing credit and other reports on consumers), the Video Privacy Protection Act, 18 U.S.C. §§ 2710–2711 (1994) (barring video stores from disclosing information), the Family Educational Rights and Privacy Act (so-called “Buckley Amendment”), 20 U.S.C. § 1232g (1994) (regulating information provided by educational institutions), the Employee Polygraph Protection Act, 29 U.S.C.A. §§ 2001–2009 (West Supp. 1999) (limiting employers’ ability to use lie detectors), the Telemarketing Protections Act, 47 U.S.C. § 227 (1994) (limiting use of automatic-dialing machines

while some personal information cannot be sold, most other commercial uses of personal information are not regulated at all.⁴⁹ For example, suppose that a bookstore and a videotape rental store, realizing that people often wish to see movies adapted from novels they have read, entered into an agreement. Under the agreement, the bookstore would provide to the video store names of customers who have purchased books which had been made into movies. The video store, in turn, would provide the bookstore with names of customers who have rented movies adapted from novels. At present, federal law prohibits video rental stores from knowingly disclosing the titles of movies rented by their customers, but nothing prevents bookstores from revealing the names and purchases of their patrons.⁵⁰ Similarly, if the customers paid for the videos with credit cards, no federal law would bar credit-card issuers from disclosing that the customers

in telemarketing), and the Cable Communications Policy Act, 47 U.S.C. § 551(a) (1994) (cable television). According to Dorothy Glancy:

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.

Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 *Computer & High Tech. L.J.* 151, 170–71 (1995); *see also* Reidenberg, *supra* note 17, at 209–10 (“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.”) (footnote omitted). *See generally id.* at 210–36 for Professor Reidenberg’s review of various privacy laws.

49. For example, cable television operators cannot disclose what shows their viewers have watched on Pay-Per-View. *See* 47 U.S.C. § 551 (1994). 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.

50. *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 than they can find out what movies you rent at the video store.” Sheryl G. Stolberg, *Privacy Concerns Delay Medical I.D.’s*, *N.Y. Times*, Aug. 1, 1998, at A10.

had done so.⁵¹ These distinctions, as well as others, make little sense.⁵²

Legal scholars and others have responded to this privacy bramble bush in a number of ways. Some have used the theories of law and economics.⁵³ Others have analyzed the problems created under traditional privacy doctrines or suggested rules to regulate data collection.⁵⁴ Still others have articulated broad principles intended to govern data collection, often focusing exclusively or largely on fairness considerations.⁵⁵ The impact of foreign laws—chiefly the European Union Data Protection Directive — on data collection in the United States has also been a topic of discussion.⁵⁶ But few have explored how consumers behave or what insights might be gleaned from laws governing other consumer/merchant transactions. The purpose of this Article is to bring to bear on privacy issues some principles and policies drawn from existing consumer-protection regulations and, to some

51. See Schwartz & Reidenberg, *supra* note 1, at 270. 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 Ann. § 59.1- 442 (Michie 1992), while California requires credit card issuers to allow credit card holders to opt out of the disclosure of their information. See Cal. Civ. Code § 1748.12 (West 1998); see also *infra* note 386.

52. Similarly, your cable television company may not lawfully communicate to others what channels you watch under 47 U.S.C. § 551, but nothing prevents your local movie theater 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 *Privacy and the NII*, *supra* note 4, at 16–17.

53. See, e.g., Murphy, *supra* note 35; Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393 (1978).

54. See, e.g., Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 Computer & High Tech. L.J. 431 (1993); Reidenberg, *supra* note 17; Reidenberg, *supra* note 4.

55. See, e.g., Privacy Working Group, Information Infrastructure Task Force, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* 6–7 (1995) [hereinafter *Privacy and the National Information Infrastructure*] (stating that users of information should disclose their purposes).

56. 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’y Int’l Bus. 275 (1998). For a thorough discussion of the extent to which U.S. laws meet European standards, see Schwartz & Reidenberg, *supra* note 1.

extent, the literature on consumer behavior and consumer transactions.

Part I of this Article discusses the benefits derived from the sale of personal information. Part II focuses on consumers' "taste" for privacy—why they care about privacy, and how much. Part III explores the discrepancy between what consumers say and what they do in fact; more specifically, if consumers say they care about privacy, and in some circumstances act to protect their privacy, why do so few of them opt out of marketing solicitations? Part III argues that marketers have both the incentives and the ability to increase consumers' transaction costs in protecting their privacy; and that some marketers do, in reality, inflate these costs. Part III also argues that many consumers, faced with significant transaction costs and other common constraints, decide not to protect their privacy. Part IV of this Article suggests and discusses ways to reduce consumers' transaction costs.

I. THE BENEFITS FROM THE TRADE IN INFORMATION

A. *Information Seekers*

1. *Commercial Interests*

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

The second use of information, marketing, differs significantly from consumer-initiated transactions. When a consumer applies for something, the merchant may require certain financial information to decide whether or not to grant the consumer's request. However, when engaged in marketing, the merchant seeks the information, generally without the consumer's knowledge, as part of the

merchant's own sales efforts.⁵⁷ Though the consumer may ultimately accept the merchant's offer, it is the merchant, not the consumer, who initiates the process by seeking information about the consumer.

The use of computer databases for marketing purposes can take many forms. In one form, businesses sell their customer lists to other companies, typically so that the purchasing companies can solicit those whose names appear on the lists.⁵⁸ List sellers find such sales highly remunerative because few additional costs are involved in selling lists that already exist and are being maintained for other purposes.⁵⁹ Indeed, with profit margins of up to sixty percent, some companies reportedly earn more from selling customer lists than from selling their own goods or services.⁶⁰ Companies have even been pursued by merger partners because of their lists.⁶¹

Another form of marketing is called prescreening. A lender who wishes to promote its credit card may ask a credit bureau to identify people who meet certain criteria specified by the lender, such as prompt bill payment and high income level. The credit bureau may supply the lender with the names of those who meet the criteria, or it may mail the lender's solicitation directly. Under this prescreening process, the lender never sees the names of those who do not meet its criteria. Those who pass the test, on the other hand, know only that they have been selected to receive the mailing; those who do not satisfy the

57. 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." Gandy, *supra* note 9, at 88.

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

59. See *id.* at 106 (quoting list manager as saying, "List rentals are almost all gravy.").

60. See Headden, *supra* note 5, at 45; Smolowe, *supra* note 17, at 66.

61. See Schwartz & Reidenberg, *supra* note 1, at 336-37 (stating that 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).

criteria will likely never find out that they were considered unfit.⁶²

Some businesses use computers for sophisticated marketing ventures. Supermarkets, for example, 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 families with small children discounts on diapers.⁶³ Supermarkets can even encode the coupons to determine who responded to which coupons, information that may be useful in future marketing attempts.⁶⁴ Some major corporations reportedly monitor consumer purchases both to bombard consumers with solicitations and to sell the information to others.⁶⁵

These marketing endeavors are far from insignificant to businesses. A 1996 Gallup poll found that seventy-seven percent of companies use direct marketing.⁶⁶ The total amount spent on mailing lists is said to run \$3 billion a

62. See generally Sheldon Feldman, *The Current Status of the Law Governing Prescreening, Including Permissible Postscreening Practices*, 46 Bus. Law. 1113 (1991). Prescreening is now regulated by the Fair Credit Reporting Act, which permits prescreening, subject to certain safeguards, and requires consumer reporting agencies to allow consumers to have their names removed from lists maintained for prescreening. See 15 U.S.C. §§ 1681b(e), 1681m(d) (Supp. IV 1998).

63. See *The Supermarket as Selling Machine*, 58 Consumer Rep. 560, 560 (1993).

64. See Marx, *supra* note 36, at 90, 91–92; Mendel-Black & Richards, *supra* note 30. Mendel-Black and Richards also describe the following:

Sharper Image . . . keeps one list of its own 800,000 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.

65. See, e.g., Foxman & Kilcoyne, *supra* note 25, at 110 (“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*, N.Y. Times, July 31, 1988, § 3 at 1.

66. See *Report to the Congress*, *supra* note 27, at 7.

year.⁶⁷ According to one estimate, direct-marketing-generated electronic commerce could rise to \$30 billion by 2002.⁶⁸ The direct-marketing industry reportedly employs more than eighteen million people,⁶⁹ and the business is growing at a rate estimated at twice that of the United States' gross national product.⁷⁰

2. Noncommercial Interests

One reason 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?⁷¹ But consumers seek access to data for other reasons too, some of which are easier to justify than others. For example, information services have helped find abducted children,⁷² deadbeat dads,⁷³ and spouses who have disappeared, leaving their

67. See William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 Fordham L. Rev. 951, 956 (1996).

68. See *Protecting Consumers Against Cramming and Spamming: Hearings Before the Subcomm. on Telecomm., Trade, & Consumer Protection of the House Comm. on Commerce*, 105th Cong. 9–104 (1998) [hereinafter *Cramming and Spamming Hearings*] (testimony of Jerry Cerasale, Senior Vice-President of Government Affairs, Direct Marketing Association, Inc.).

69. See Fenrich, *supra* note 67, at 956.

70. See Arthur M. Hughes, *The Complete Database Marketer* 5 (rev. ed. 1996) ("It is and will continue to be the hottest growth area in advertising for the foreseeable future.").

71. See, e.g., *Jones v. Federated Fin. Reserve Corp.*, 144 F.3d 961 (6th Cir. 1998) (involving person who obtained credit report on roommate's ex-spouse); *Yohay v. City of Alexandria Employees Credit Union*, 827 F.2d 967 (4th Cir. 1987) (involving person who obtained credit report on ex-spouse); Privacy Rights Clearinghouse, *Second Annual Report of the Privacy Rights Clearinghouse* 40–41 (1995) (describing parents who checked on son's fiancée); Gini G. Scott, *Mind Your Own Business* 325 (1995) ("[P]eople check up on neighbors, friends, dates, mates, family members, and others."); Chandrasekaran, *supra* note 17 (describing college students using Lexis-Nexis to check on dates' ages and marital status).

72. See FTC, *Session One: Database Study*, *supra* note 21, at 229 (remarks of Bruce Hulme, Legislative Committee Member of National Council of Investigation and Security Services) (describing service that helped locate over 2000 abducted children).

73. See FTC, *Public Workshop on Consumer Privacy Session One: Computerized Databases Containing Sensitive Consumer Identifying Information* (visited Oct. 6, 1999) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments1/aces2.htm>> (remarks of Geraldine Jensen, President, Association for Children for Enforcement of Support, Inc.) (reporting that service has assisted over 25,000 families in locating absent parents who owe child support; average family collected \$4000 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).

husbands or wives with jointly incurred debts.⁷⁴ Long-lost relatives and important trial witnesses have also been found through Internet services.⁷⁵

On the other hand, some use computers as an adjunct to unlawful acts, such as stalking.⁷⁶ Abusive husbands have employed the Internet to hunt fleeing wives. Similarly, criminals have used the Internet to steal identities.⁷⁷ Obviously, such uses can pose serious problems and should not be indulged under any circumstances.

B. *Benefits to Consumers*

Consumers may also benefit from having their names appear in databases. In fact, some are so persuaded by these benefits they are willing to pay to appear in certain databases.⁷⁸ The benefits, whether real or potential, are numerous. First, many consumers make purchases through direct-marketing channels.⁷⁹ More than half the respondents to a 1996 Equifax survey said that they or someone in their household had recently bought something from a mailing.⁸⁰ Fourteen percent of the respondents to a 1990 survey had purchased something offered to them in telephone calls.⁸¹ Indeed, consumers reportedly bought approximately \$600 billion worth of

74. See Rothfeder, *supra* note 10, at 106–12.

75. For examples, see the stories collected at Switchboard Inc., *True Stories About Switchboard Bringing People Together* (visited Oct. 6, 1999) <<http://www.switchboard.com/stories.htm>>; see also Chandrasekaran, *supra* note 17, at A1; FTC, *Session One: Database Study*, *supra* note 21, at 6 (remarks of FTC Chairman Robert Pitofsky) (“[D]atabases have been critical in locating witnesses, tracking down criminals, and even reuniting lost family members.”).

76. For a chilling account of the role of computers in the stalking and eventual murder of actress Rebecca Schaeffer, see Rothfeder, *supra* note 10, at 13–15.

77. See Center for Public Integrity, *supra* note 32, at 7.

78. See *infra* notes 369–71 and accompanying text.

79. See Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 Harv. J.L. & Pub. Pol’y 591, 599 (1994) (“Many consumers enjoy receiving mailings and shopping at home.”).

80. See *Equifax-Harris Consumer Privacy Survey* 18 (1996) [hereinafter *1996 Equifax Survey*]; see also *1990 Equifax Report*, *supra* note 45, at 68 (reporting similar findings; additionally, 16% 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 who stated that over 100 million Americans had shopped at home in some form in previous year).

81. See *1990 Equifax Report*, *supra* note 45, at 68.

goods and services through direct-marketing channels in 1995.⁸²

Second, consumers whose interests are correctly identified by sellers may incur lower overall search costs.⁸³ For example, a consumer who wishes to purchase a new computer might be grateful to receive an unsolicited computer catalog in the mail because the catalog could save him or her 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, thus reducing unwanted solicitations.⁸⁴ If sellers are deprived of consumer information, some say, they will respond by soliciting all consumers, not just those who might be interested in their products or services.⁸⁵ Response rates to mailings have risen in recent years, suggesting that direct marketers have improved their ability to identify likely buyers.⁸⁶

This argument is flawed. Even if response rates have risen to five percent, that still leaves ninety-five percent of uninterested recipients, many of whom would rather not

82. See *Private Ayes*, Marketing Tools, Jan.–Feb. 1996, at 31. This number is projected to grow at a rate of 7.2% a year. See Neil Munro, Washington Tech., *Putting a Price on Technology* (Mar. 6, 1997) <http://www.wtonline.com/archive/97-03-06/front_page/putting_link.html>.

83. See Anthony T. Kronman, *The Privacy Exemption to the Freedom of Information Act*, 9 J. Legal Stud. 727, 747 (1980); Daniel Klein & Jason Richner, *In Defense of That Pesky Junk Mail*, Chi. Trib., 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.”).

84. The argument is presented and criticized in Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. 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.

85. 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 Three: Consumer Online Privacy* (June 12, 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/index.html>> [hereinafter FTC, *Session Three: Online Privacy*] (remarks of Jason Catlett, Chief Executive Officer, Junkbusters Corp.) (stating that 10,000 pieces of spam cost one dollar to send).

86. See Foxman & Kilcoyne, *supra* note 25, at 108; Richard Lacayo, *Nowhere to Hide*, Time, Nov. 11, 1991, at 37.

have gotten the offer.⁸⁷ Indeed, the cost of nonconsensual databases—in terms of unread mailings and unwanted telephone solicitations—is estimated to approach \$50 billion.⁸⁸ The argument also assumes that businesses would not respond to the loss of information by adopting a cheaper alternative to direct-mail advertising. Finally, the argument presupposes that other methods of reducing junk mail cannot be devised.

Fourth, consumers with good credit records, who wish to borrow, benefit from lender access to their financial information. If lenders could not determine consumers' credit-worthiness, they may charge consumers higher interest rates to compensate for the risk of lending to persons with no credit history. Other lenders may simply reject such loans.⁸⁹

Fifth, some products may not even be available but for computer databases. These databases furnish information needed for marketing research, and in the absence of such research, some sellers may decide against incurring the risks and expenses of introducing new products.⁹⁰

Sixth, the use of computer databases in marketing makes it possible, at least theoretically, to sell products at lower prices.⁹¹ If sellers believe that the cost of using

87. See Foxman & Kilcoyne, *supra* note 25, at 108. Response rates to telemarketing are said to be even higher than for direct mail. See Caroline E. Mayer, *Telemarketers Just Beginning to Answer Their Calling*, Wash. Post, Aug. 31, 1997, at H1.

88. See Kenneth C. Laudon, *Markets and Privacy*, 39 Comm. of the ACM 92, 103 (1996).

89. See Judith B. Prowda, *Privacy and Security of Data*, 64 Fordham L. Rev. 738, 751 (1995).

90. See Goodwin, *supra* note 47, at 159:

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*, Eur. Res., May 1987, at 78.

91. See, e.g., David J. Klein, Comment, *Keeping Business out of the Bedroom: Protecting Personal Privacy Interests from the Retail World*, 15 J. Marshall J. Computer & Info. L. 391, 393 n.10 (1997) (“Some companies can offer discounts on their goods when they utilize personality

databases is cheaper than other means, they will continue to use databases in their marketing efforts. The average return for a dollar spent on direct-mail advertising is ten dollars, more than twice the return when compared with television commercials.⁹² The average mailing generates ten times the response produced by a newspaper ad and 100 times the response from a television commercial.⁹³ Hence, more money is spent on direct mail than on magazine ads, radio commercials, or television pitches.⁹⁴ If sellers were denied access to databases, they would be forced to employ more expensive selling methods—measured by the cost-per-sale—or else, if alternative methods prove to be too costly, forgo selling the product altogether.⁹⁵ If the cost-per-sale increases, it is likely that the price of the product will also increase. Consequently, those who wish to buy the product will have to pay a higher price for it—in essence, paying to protect the privacy of others.⁹⁶

In sum, the use of computer databases to maintain information on consumers has its benefits.⁹⁷ Some claim that because businesses have a stake in the outcome of privacy discussions, they would tend to inflate the benefits generated by databases and underestimate the costs

profile lists, because they send fewer mail advertisements, and they send them only to those persons who are likely to purchase the product.”).

92. See Headden, *supra* note 5, at 42, 44.

93. See Smolowe, *supra* note 17, at 65.

94. See *id.* at 63.

95. See Goodwin, *supra* note 47, at 159 (“[S]mall business owners in Alaska claimed they need access to tourism mailing lists to carry out successful promotion and promote entrepreneurial development.”); *What Price Privacy?*, *supra* note 30, at 359 (“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% and increase the response rate too. ‘For us,’ he says, ‘that spells the difference between making a solid profit or closing our doors.’”).

96. Some also claim that mail-order selling reduces damage to the environment because it enables people to shop without traveling. See Bibas, *supra* note 79, at 600; Prowda, *supra* note 89, at 751; Klein & Richner, *supra* note 83, at 19. But see *infra* note 120 and accompanying text for argument that direct-mail solicitations damage the environment.

97. See Goodwin, *supra* note 47, at 159 (“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.”).

databases produce.⁹⁸ While this is a credible argument, it seems clear that some consumers do value the trade in personal information, even if the benefits are somewhat exaggerated.

II. THE TASTE FOR PRIVACY

A. *Why Do People Care About Privacy?*

In a number of articles, Judge Richard Posner (then a law professor) attempted to construct an economic theory of the right to privacy.⁹⁹ Posner focused on privacy as an intermediate goal. In his view, regarding privacy purely as a consumption good “would bring the economic analysis to a grinding halt because tastes are unanalyzable from an economic standpoint.”¹⁰⁰ 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 that would “correct misapprehensions that the individual is trying to exploit,”¹⁰¹ such as the fact that one had previously defaulted on a loan.

Many consumers, however, seem to reject this view of privacy. In one survey, sixty-four percent of respondents disagreed with the statement, “Most people who complain about their privacy are engaged in immoral or illegal conduct.”¹⁰² Viewing privacy as an end in itself, rather than

98. See Foxman & Kilcoyne, *supra* note 25, at 108.

99. See Richard A. Posner, *An Economic Theory of Privacy*, Regulations, May/June 1978, at 19; Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 Buff. L. Rev. 1 (1979); Posner, *supra* note 53. 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 also appears at *Symposium: The Law and Economics of Privacy*, 9 J. Legal Stud. 621–842 (1980), with a brief introduction by Judge Posner.

100. Posner, *supra* note 53, at 394.

101. *Id.* at 399. In a later piece, Judge Posner wrote that the desire to protect against embarrassment 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).

102. Priscilla M. Regan, *Legislating Privacy* 48 (1995).

as a means to an end, may retard analysis in some respects. But an economic theory that overlooks those who value privacy as an end in itself is necessarily incomplete.¹⁰³

What is behind the taste for privacy? Alan Westin has speculated that it may be biological in origin.¹⁰⁴ In fact, some commentators have noted that privacy is so fundamental to life that few pleasures can survive without it.¹⁰⁵ Available literature on psychology, though sparse, suggests that the desire for privacy may stem from a number of motives.¹⁰⁶

Deep feelings can be generated by privacy invasions. Arthur Miller has observed that “[s]ome 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.”¹⁰⁷ For example, the incontinent women who requested free samples¹⁰⁸ 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 humiliation if others find

103. 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. . . . [P]rivacy 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.

Id.; see also Anthony D'Amato, *Comment: Professor Posner's Lecture on Privacy*, 12 Ga. L. Rev. 497, 499 (1978).

104. See Alan F. Westin, *Privacy and Freedom* 8–11 (1967).

105. See Fried, *Privacy*, *supra* note 45, at 477 (“[Privacy] is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. . . . [W]ithout privacy they are simply inconceivable.”). For a discussion of the philosophical underpinnings of privacy doctrine, see Regan, *supra* note 102, at 24–33.

106. See Cathy Goodwin, *A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption*, 1 J. Consumer Psychol. 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.”).

107. Arthur R. Miller, *The Assault on Privacy* 48–49 (1971).

108. See *supra* note 37 and accompanying text.

out.¹⁰⁹ 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.”¹¹⁰ In Richard Murphy’s words, “In the utility calculus, these psychic values count.”¹¹¹

Some consumers with a taste for privacy may be concerned about the loss of control over their personal information. Consumers engaged in transactions that appear limited in scope may provide information that ends up being used for purposes far beyond those intended by the original transactions. A child who celebrates a birthday at an ice cream store may unwittingly become an entry in a database.¹¹² Similarly, most consumers object to others finding out about their income or how much their homes are worth.¹¹³ Consumers may also wish to keep certain information private to prevent access to other personal information. For example, someone who knows your Social Security number and your mother’s maiden name may be able to learn your bank account balance.¹¹⁴

109. See *Privacy and the NII*, *supra* note 4, at 3 (“[A]n individual may want to keep certain types of health data confidential from the general public because its disclosure could cause the person embarrassment.”). According to Anthony Kronman:

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.

Anthony T. Kronman, *The Privacy Exemption to the Freedom of Information Act*, 9 J. Legal Stud. 727, 746–47 (1980) (footnote omitted) (emphasis in original).

110. Reidenberg, *supra* note 4, at 498. For a discussion of the role of dignity in privacy, see Kang, *supra* note 84, at 1259–65.

111. Murphy, *supra* note 35, at 2386.

112. See Goodwin, *supra* note 47, at 152.

113. See Hal R. Varian, *Economic Aspects of Personal Privacy*, in *Privacy and Self-Regulation in the Information Age* (visited Oct. 6, 1999) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>>.

114. See *Privacy and the NII*, *supra* note 4, at 3. 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 Fried, *Privacy*, *supra* note 45.

Some consumers 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.¹¹⁵ Others are concerned about identity theft.¹¹⁶

Consumers object to unwanted solicitations for a number of reasons. Some merely want to be left alone—who has not been annoyed by a telephone solicitation at dinnertime? Many find intrusions in the home particularly irritating. Consumer law has been especially responsive to this concern, often providing legal protections to consumers solicited in their homes.¹¹⁷

Even unwanted mail solicitations are troubling. It has been estimated that the average professional in the United States will spend eight months sorting junk mail over the course of his or her lifetime.¹¹⁸ Some consumers complain that important mail has gotten lost in the flood of junk mail.¹¹⁹ Environmentalists have claimed that junk mail makes up three percent of the nation's landfills.¹²⁰ According to one estimate, the average American received 553 junk mail in 1997, totaling 4.5 million tons for the entire country.¹²¹

Some consumers are also concerned about the volume of commercial e-mail messages. America Online (AOL) receives thousands of complaints about unsolicited

115. See Mark Lewyn, *You Can Run, But It's Tough to Hide from Marketers*, Bus. Week, Sept. 5, 1994, at 60 (family of police officer).

116. See Edmund Mierzwinski, *Data Dealers Seizing Control of Our Lives*, 19 *At Home with Consumers* 4 (1998) (“[U]nrestricted 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.”).

117. 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. § 429.1 (1999). Some states have enacted similar statutes. See, e.g., N.Y. Pers. Prop. Law § 425 (West 1998). Some states have even enacted such statutes for telephone sales; a list appears in Dee Pridgen, *Consumer Credit and the Law* app. 15A (1994).

118. See Smolowe, *supra* note 17, at 63.

119. See *id.* at 67.

120. See *id.* at 64.

121. See Evan Hendricks, *Capital Insights*, Privacy Times, Dec. 15, 1997, at 1.

commercial e-mails every day,¹²² making it by far the most frequent subject of complaint by AOL subscribers.¹²³ Depending on the day of the week, between five percent and thirty percent of the e-mails received by AOL subscribers consists of unsolicited commercial e-mails.¹²⁴ Some recipients of commercial e-mail messages end up incurring unwanted expenses because some Internet service providers charge customers more for receiving additional messages.¹²⁵

Businesses may also benefit from satisfying consumers' privacy interests. Thus, a number of commentators and 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.¹²⁶ Polls have reported that

122. See *Cramming and Spamming Hearings*, *supra* note 68 (testimony of Randall Boe, Associate General Counsel, America Online, Inc.).

123. See FTC, *Public Workshop on Consumer Information Privacy Session Two: Consumer Online Privacy* (June 12, 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/index.html>> [hereinafter *FTC, Session Two: Consumer Online Privacy I*] (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, Georgia Institute of Technology) (reporting that 74% of respondents to survey disagreed strongly that they liked receiving mass e-mailings); Center for Democracy & Tech., *Preliminary Comments to the Federal Trade Commission on Unsolicited Commercial E-mail* (June 2, 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/votele.htm>> (responding 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").

124. See FTC, *Session Two: Consumer Online Privacy I*, *supra* note 123, at 48 (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) (reporting that nonrepresentative survey of Internet users found that for about one-third of those surveyed, spam made up one-quarter of e-mail).

125. See *Cramming and Spamming Hearings*, *supra* note 68, at 4 (testimony of Paula Selis, Senior Counsel, Consumer Protection Division, Washington State Attorney General's Office); see also Voters Telecomm. Watch, *Final Comments to the FTC on Unsolicited Commercial Email*, (visited Aug. 21, 1998) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/ftcfilin.htm>> [hereinafter *Final Comments*] (reporting that of over 2700 people surveyed, 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).

126. See, e.g., FTC, *Privacy Online*, *supra* note 39, at 43 ("If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential."); Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. Rev. 847, 851 (1998); John V. Swinson, *Confidentiality on the*

privacy is the top reason why some consumers have declined to use the Internet.¹²⁷

B. How Much Do People Say Privacy Matters to Them?

Over the last decade, numerous polls—many of them conducted by Equifax and Alan Westin—have fleshed out what consumers think about privacy. On some privacy issues, consumers are united, often taking pro-privacy positions. But many consumers have also concluded that other values are more important than privacy. On other privacy issues, consumers are divided. Even then, however, large percentages of them take pro-privacy positions.

1. Issues on Which Consumers Tend to Agree

According to a 1996 survey commissioned by Equifax, eighty-nine percent of the public is concerned about threats to personal privacy.¹²⁸ Similarly, results of other polls have

Superhighway, Am. Law., Dec. 1995, at 23; Amy Harmon, *F.T.C. to Call for Laws to Protect Children Online*, N.Y. Times, June 4, 1998, at D1; Evan Hendricks, *E-Commerce & Privacy*, Privacy Times, May 29, 1998, at 10 (remarks of Madeline Mooney, Vice-President, Lycos Inc.). But see Peter P. Swire & Robert E. Litan, *None of Your Business* 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.”).

127. See *Cramming and Spamming Hearings*, supra note 68. (statement of the FTC on consumer privacy) (“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.”); see also Evan Hendricks, *House Hearing Covers Self-Regulation, Encryption*, Privacy Times, Apr. 3, 1998, at 2, 3; Evan Hendricks, *Internet Users Want New Privacy Laws, Survey Finds*, Privacy Times, Jan. 2, 1997, at 4, 5; Letter of Jerry Berman & Deirdre Mulligan, Executive Director and Staff Counsel, Center for Democracy & Tech., to FTC (visited Oct. 6, 1999) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/demotech.htm>>; eTRUST, *Comments of eTRUST Concerning Consumer On-Line Privacy* (visited Oct. 6, 1999) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/etrust.htm>>; Family PC, *Kids’ Safety & Parental Guidance Clearinghouse* (visited Oct. 6, 1999) <<http://www.zdnet.com/familypc/content/kidsafety/results/html>>.

128. See Alan F. Westin, “Whatever Works”: *The American Public’s Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, in *Privacy and Self-Regulation in the Information Age*, (visited Oct. 6, 1999) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>> [hereinafter Westin, *Whatever Works*]. That number has increased slowly but steadily. For example, in 1994, 84% of those surveyed stated that they were concerned, up from 79% in 1990 and 77% in 1983. See *Equifax-Harris Mid-Decade Consumer Privacy Survey* 17 (1995)

confirmed that many consumers are concerned about their privacy.¹²⁹ Increasingly, more and more consumers agree that they have “lost all control over how personal information about them is circulated and used by companies.”¹³⁰ Nearly four out of every five respondents regard privacy as a fundamental right, worthy of addition to the list in the Declaration of Independence of “life, liberty and the pursuit of happiness.”¹³¹ One poll found that ninety-eight percent of respondents believe that their privacy is being substantially threatened by marketers and advertisers.¹³²

Consumers are also in accord on other issues. For example, ninety-seven percent of parents whose children use the Internet believed that web sites should not sell or rent personal information relating to children.¹³³ Nearly three-quarters found it objectionable for a web site to request a child’s name and address even if used solely for internal purposes.¹³⁴ A 1991 survey found that more than

[hereinafter *Equifax Mid-Decade Survey*]; 1990 *Equifax Report*, *supra* note 45, at 2. The 1995 figure was 82%. See *Equifax Mid-Decade Survey*, at 17. Similarly, one 1998 survey found that 87% of computer users were concerned. See Alan F. Westin & Danielle Maurici, *E-Commerce & Privacy: What Net Users Want 7* (1998). Similarly, another survey conducted in the same year found that 88% of consumers were concerned. See *Executive Summary: 1998 Privacy Concerns and Consumer Choice Survey* (visited Dec. 17, 1998) <<http://www.privacyexchange.org/iss/surveys/1298execsum.html>> [hereinafter *1998 Executive Summary*].

129. The Cambridge Reports surveys, conducted in 1988 and 1989, found that more than two-thirds of the respondents considered personal privacy “very important” and nearly a quarter called it “somewhat important.” James E. Katz & Annette R. Tassone, *Public Opinion Trends: Privacy and Information Technology*, 54 *Pub. Opinion Q.* 125, 135, 139 – 40 (1990). More than two-thirds of those queried were either “very concerned” or “somewhat concerned” about invasion of their personal privacy. *Id.* 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. See Ann Reilly Dowd, *Money Poll: You’re Deeply Worried About Your Privacy*, *Money*, Aug. 1, 1997, at 107.

130. Westin, *Whatever Works*, *supra* note 128, at 56 (71% in 1990; 80% in 1995; 83% in 1996).

131. 1990 *Equifax Report*, *supra* note 45, at 7.

132. See Mary J. Culnan, *Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing*, 9 *J. Direct Marketing* 10, 11 (1995) (describing survey conducted by Yankelovich Partners, Inc.).

133. See FTC, *Privacy Online*, *supra* note 39, at 6.

134. See *id.* 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 Mark S. Ackerman et al., AT&T Labs, *Beyond Concern:*

half of the respondents believed that it is important to allow consumers to opt out of the sale of personal information, while one-third viewed it as somewhat important.¹³⁵ Consumers also dislike telephone solicitations; forty-seven percent of respondents indicated that telephone solicitations are “always an intrusion,” while thirty-two percent found such solicitations to be “mostly an intrusion.”¹³⁶

Although people acknowledge the importance of privacy, most value other things even more. 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.¹³⁷ Similarly, ninety-six percent of respondents agree that “when people want to borrow money, the company giving them credit should be able to check on their credit records”¹³⁸ Additionally, a substantial majority find it acceptable for companies to check the public records for information on those who apply for auto insurance or jobs.¹³⁹ Therefore, consumers seem willing to permit the use of private information to facilitate certain transactions.

2. *Issues on Which Consumers Are Divided*

Several polls have made it clear that some consumers have more of a taste for privacy than others.¹⁴⁰ For example, the 1990 Equifax Report compared certain demographic characteristics with the answers given by respondents to forty-six questions. Equifax found that liberals were more privacy-oriented than moderates and

Understanding Net Users' Attitudes About Online Privacy (visited Apr. 19, 1999) <<http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm>>.

135. See *Harris-Equifax Consumer Privacy Survey* 19 (1991) [hereinafter *1991 Equifax Survey*].

136. *1998 Executive Summary*, *supra* note 128.

137. See *1990 Equifax Report*, *supra* note 45, at 26.

138. *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.*

139. See *Harris-Equifax Consumer Privacy Survey* 5 (1992).

140. See *1990 Equifax Report*, *supra* note 45.

conservatives on twenty-three of the questions; Jews were more privacy-oriented than Protestants and Catholics on thirty-two of the questions; and those who had read and heard about consumer privacy issues in the previous year were more privacy-oriented on eighteen questions than those who had not read or heard about such issues.¹⁴¹ The desire for privacy also varied by age¹⁴² and by experience with computers.¹⁴³ Another survey found that women tend to be more concerned about threats to their privacy—including privacy on the Internet¹⁴⁴—than are men.¹⁴⁵ Notwithstanding Judge Posner's view, the most plausible 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 differences in preferences for privacy suggest that any rule designed to accommodate the preferences of different consumers on various issues will need to be flexible.

Many consumers are troubled by the trade in personal information. The 1990 Equifax survey showed that while thirty-nine percent of respondents viewed the sharing of information by companies in the same industry as a major problem, forty-three percent called it a minor problem, and sixteen percent said it was not a problem at all.¹⁴⁶ Similarly, although fifty-seven percent felt that consumers' being asked to provide excessively personal information is a major problem, thirty-three percent described it as only a minor problem, and ten percent did not perceive a problem at all.¹⁴⁷ A 1996 survey found that half of the public was

141. *See id.* at xxv.

142. *See id.*

143. *See id.* at xxv–xxvi.

144. *See* FTC, *Public Workshop on Consumer Information Privacy Session Two: Consumer Online Privacy* (June 11, 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/index.html>> [hereinafter FTC, *Session Two: Consumer Online Privacy II*] (remarks of Humphrey Taylor, Chairman and Chief Executive Officer, Louis Harris & Associates, Inc.).

145. *See* Dowd, *supra* note 129 (stating that 80% of women are concerned about threats to their privacy, while only 68% of men are similarly concerned).

146. *See* 1990 *Equifax Report*, *supra* note 45, at 18.

147. *See id.*

not concerned or only slightly concerned about having their names appear on mailing lists, while the other half was somewhat concerned or greatly concerned.¹⁴⁸

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 would like to get mailings on products and services of interest to them.¹⁴⁹ In 1996, thirty-seven percent of respondents to an Equifax poll said that they regard mail offers as a nuisance, while forty-three percent reported that they do not see them as a problem, although they rarely use them. Twelve percent regarded mail offers as “primarily a useful opportunity.”¹⁵⁰ The survey also found that fifty-five percent of the public felt that compiling profiles of individual consumers’ purchasing patterns and using those profiles to solicit consumers are somewhat acceptable. Another eleven percent believed such profiling to be very acceptable, while a third viewed it as either not very acceptable, or not at all acceptable.¹⁵¹ Similarly, in 1990, only twenty-three percent said they would be very or somewhat upset if they could not receive offers of credit by mail or telephone, while twenty-one percent said they would not be very upset, and fifty-six percent said they would not be upset at all.¹⁵²

Although nearly all consumers who receive unsolicited commercial e-mails dislike them, they differ in the intensity

148. See Beth Negus, *You’re Not Welcome; Direct Survey Has Alarming Findings About ‘Junk’ Views and Data Protection*, Direct, June 15, 1996, at 1, 60 (reporting that 27% were not at all concerned, 23% were slightly concerned, 24% were somewhat concerned, and 25% were greatly concerned).

149. See *id.* at 61. 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. See *id.* at 64; see also *1990 Equifax Report*, *supra* note 45, at 28 (reporting that 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).

150. *1996 Equifax Survey*, *supra* note 80, app. A at 8. In 1991, 46% saw mail offers as a nuisance, 38% rarely used them but did not see a problem, and 6% regarded them as useful. See *id.*; *1991 Equifax Survey*, *supra* note 135, at 16–17.

151. See *1996 Equifax Survey*, *supra* note 80, at 84.

152. See *1990 Equifax Report*, *supra* note 45, at 30.

of their reactions. One survey found that forty-two percent of respondents felt that unsolicited e-mails are “getting to be a real pain and [they] want to stop getting these messages,” while fifty-five percent—less critical—viewed the e-mails as a little bothersome. Only three percent liked receiving the messages.¹⁵³ A 1996 survey found forty-three percent of Internet users disagreed strongly that online providers should be able to track their Internet use in order to send them targeted offers. Twenty-eight percent disagreed somewhat, while a quarter agreed somewhat and four percent agreed strongly.¹⁵⁴

This variation in views is also shared by executives in privacy-intensive industries, people who are likely to know more than ordinary consumers about the extent to which consumer information is available. The 1990 Equifax report indicated that these executives are terribly conflicted about whether the privacy of personal information stored in computers is adequately safeguarded. Depending on the industry, the range of executives who thought it was adequately safeguarded varied from thirty-nine percent to fifty-seven percent, while the percentages of those who thought it was not adequately safeguarded ranged from forty percent to fifty-seven percent.¹⁵⁵

Some survey results may have been affected by the manner in which the questions were posed. Even taking this factor into consideration, however, it is quite clear from the survey results that while many consumers are troubled by the availability of information about them, others do not seem troubled. Some even expressed an appreciation for the major consequence of the trade in consumer

153. See FTC, *Session Two: Consumer Online Privacy II*, *supra* note 144, at 10 (remarks of Humphrey Taylor, Chairman and Chief Executive Officer, Louis Harris & Associates, Inc.); see also Alan F. Westin et al., *Commerce, Communication, and Privacy Online* 23 (1997); Ackerman et al., *supra* note 134 (reporting that 52% of unrepresentative sample found unsolicited commercial e-mail very serious); *Final Comments*, *supra* note 125.

154. See *1996 Equifax Survey*, *supra* note 80, at 71.

155. See *1990 Equifax Report*, *supra* note 45, at 85. Similarly, a poll of 342 chief information officers found that, in their personal use of the Internet, 60% were not willing to give up their privacy in exchange for added customer value or convenience. See CIO Comm., Inc., *CIOs Grapple with Double Standard on Internet Privacy Regulations* (visited Apr. 13, 1999) <<http://www.cio.com/knowpulse/perspectives99>>.

information—namely, receiving solicitations at home. Thus, the surveys seem to indicate that consumers are divided.

The survey results have led Alan Westin to divide consumers into three groups.¹⁵⁶ Westin describes about twenty-four percent 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.¹⁵⁷ Westin identifies as “Privacy Unconcerned” people who have little problem supplying personal information to organizations. This group, estimated to comprise about sixteen percent of consumers, sees little need for privacy legislation.¹⁵⁸ Finally, the remaining sixty percent 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 factors as whether they trust the particular industry, the individual and societal values they attach to particular uses of 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 solutions fail.¹⁵⁹

This split shows up in other ways as well. In 1990, for example, Equifax asked differently worded questions designed to elicit reactions to the sale of mailing lists. When the questions were posed in one way, sixty-nine percent said that the ability of businesses to buy mailing-list information about them is a “bad thing.”¹⁶⁰ Of these, forty percent described themselves as very concerned

156. See 1996 Equifax Survey, *supra* note 80, at 13.

157. See *id.*; see also Westin, *Whatever Works*, *supra* note 128.

158. See 1996 Equifax Survey, *supra* note 80, at 13.

159. See *id.* at 13–14; Westin, *Whatever Works*, *supra* note 128.

160. 1990 Equifax Survey, *supra* note 45, at 69. Another poll found 67% of respondents concerned about the sale of personalized marketing lists and 69% concerned about Internet companies soliciting information about their family’s buying habits. See Dowd, *supra* note 129. Still another found that 68% of consumers regard the collection and distribution of data to marketing companies as a serious invasion of privacy. See Culnan, *supra* note 132, at 11.

about privacy, while another forty-six percent were somewhat concerned. On the other hand, twenty-eight percent called sales of mailing-list information a good thing.¹⁶¹ When the question was posed another way, a two-to-one majority found the sale of mailing lists acceptable.¹⁶² It seems that one group consistently viewed the sale of information about individuals as unfortunate, regardless of how the question was phrased, another group saw it as desirable no matter how the question was put, and a third group was swayed by the wording of the question.

The 1990 Equifax surveyors also asked consumers about prescreening in two different ways.¹⁶³ When the question was put one way, about three-quarters of consumers found prescreening unacceptable, while a quarter called it acceptable.¹⁶⁴ When the survey asked

161. See 1990 Equifax Report, *supra* note 45, 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?

Id. 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?” *Id.* Similarly, an American Express telephone survey found that 80% of all Americans think that companies should not give out personal information to other companies. See Mary G. Jones, *Privacy: A Significant Marketing Issue for the 1990s*, 10 J. Pub. Pol’y & Marketing 133, 139 (1991).

162. See 1990 Equifax Report, *supra* note 45, 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?

Id.

163. For a discussion of prescreening, see *supra* note 62 and accompanying text.

164. See 1990 Equifax Report, *supra* note 45, 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

about prescreening in different words, however, respondents found it acceptable by a two-to-one margin.¹⁶⁵ Again, it appears that a hard-core of consumers viewed prescreening as acceptable, another group found it unacceptable, and a third group's view was affected by the manner in which survey questions were asked.¹⁶⁶

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.¹⁶⁷ Other surveys

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?

Id. Just 23% of the respondents answered that the practice was acceptable, while 76% found it unacceptable. *See id.*

165. *See 1990 Equifax Report, supra* note 45, 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?

Id. When put this way, 66% found the practice acceptable and 32% called it unacceptable. *See id.*

166. When Equifax asked about prescreening again in 1996, in connection with insurance, just over half the public found it “very” or “somewhat” acceptable while another quarter found it “not at all acceptable.” *1996 Equifax Survey, supra* note 80, at 11.

167. *See Westin, Whatever Works, supra* note 128. Other 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 findings supporting Westin's conclusion, see *1990 Equifax Report, supra* note 45, 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 prescreening 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

also suggest that consumers favor disclosure by companies. A 1991 survey conducted by Time Magazine and Cable News Network found that ninety-three percent of respondents agreed that the law should require companies to obtain permission from consumers before selling their personal information.¹⁶⁸ Similarly, a Money Magazine poll found that “eighty-eight percent of the public favors a privacy bill of rights that would require companies to tell consumers and employees exactly what kind of personal information they collect and how they use it.”¹⁶⁹

C. *How Do Consumers Act to Protect Their Privacy?*

Perhaps the most common way by which consumers protect their privacy is to unlist their telephone numbers. 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 unlist their numbers. The percentage of consumers willing to pay for unpublished numbers varies from state to state. In California, fifty-five percent of residential telephone numbers are unlisted, while in New York, only twenty-four percent of residents have unpublished numbers.¹⁷⁰

Other evidence indicates that some consumers value privacy highly. The 1990 Equifax report found that thirty percent of Americans decided against applying for jobs, credit, or insurance because they did not want to reveal

it as acceptable while 9% continued to view it as unacceptable. *See 1990 Equifax Report, supra* note 45, 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 preapproved offers of insurance to, 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. *See 1996 Equifax Survey, supra* note 80.

168. *See* 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. *See* Culnan, *supra* note 132, at 11.

169. *See* Dowd, *supra* note 129.

170. *See* Eli M. Noam, *Privacy and Self-Regulation: Markets for Electronic Privacy*, in *Privacy and Self-Regulation in the Information Age* (visited Oct. 6, 1999) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>>.

certain information about themselves.¹⁷¹ Although it is impossible to know precisely what information those people were trying to conceal, 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 because they were unwilling to provide the information sought signals “the unease felt by the American public concerning how personal information is used by large organizations.”¹⁷²

Similarly, the Federal Trade Commission has observed that a substantial number of consumers would rather not use certain Internet-based services when they do not know the privacy practices of those services.¹⁷³ The 1995 Equifax survey found that fifty-nine percent of the public had refused to give information to a business because they thought the information was either not needed or was too personal.¹⁷⁴ Significantly, pollsters found in 1990 that those who knew 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.¹⁷⁵

Consumers have acted in other ways to protect their privacy. Some have even tried to prevent 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.¹⁷⁶ The database, dubbed “Marketplace: Households,” would have been available at a price that small businesses and nonprofit organizations

171. See 1990 Equifax Report, *supra* note 45, at 13.

172. *Id.*; see also Foxman & Kilcoyne, *supra* note 25, at 115 (describing voter whose personal information was used as a result of voting as saying: “I have voted in every election since I was 18, and I think [this] was the last election I’ll ever vote in.”).

173. See FTC, *Privacy Online*, *supra* note 39, at 3; see also 1998 Executive Summary, *supra* note 128 (reporting that 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”).

174. See Equifax Mid-Decade Survey, *supra* note 128, at 3.

175. See 1990 Equifax Report, *supra* note 45, at 15.

176. See Mendel-Black & Richards, *supra* note 30; Sullum, *supra* note 46, at 28, 29.

could afford, and would have been extremely useful. 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."¹⁷⁷ The companies abandoned the effort after receiving some 30,000 calls, e-mails, and letters of complaint from people who were concerned about having their names included in the database.¹⁷⁸ 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 voice their concern. Consumer complaints have also caused other businesses to abandon plans that some feel would have infringed upon consumer privacy.¹⁷⁹

177. Sullum, *supra* note 46, at 29.

178. See Mendel-Black & Richards, *supra* note 30. 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. 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?*, *supra* note 30, at 360. 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." See Mary J. Culnan, *Self-Regulation on the Electronic Frontier: Implications for Public Policy*, in *Privacy and Self-Regulation in the Information Age* (visited Oct. 6, 1999) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>>.

179. See, e.g., Hendricks, *supra* note 121 (reporting that 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 (reporting that 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, at 6 (reporting that company reversed decision to sell customer names and addresses after receiving more than 75,000 customer protests); Seth Schiesel, *America Online*

III. 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 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 some consumers have permitted the use of their personal information for marketing in accordance with their preferences. At first blush, this is what Coase's famous theorem appears to predict.¹⁸⁰ Under Coase's theorem, when people can bargain freely without transaction costs—an important limitation which will be discussed below—their bargaining will produce an efficient allocation of resources regardless of which party initially possessed the relevant property right.¹⁸¹

This theorem suggests that people who value their privacy more than what the information is worth to its commercial owners would pay businesses not to keep the data.¹⁸² Conversely, if businesses value the data more than people value their privacy, people would not wish to pay businesses to stop using the data.

Backs Off Plan to Give Out Phone Numbers, N.Y. Times, July 25, 1997, at D1 (reporting that company abandoned plan to provide lists of customers' phone numbers to telemarketers and others within 24 hours after plan became widely known and consumers complained).

180. See R.H. Coase, *The Problem of Social Cost*, 3 J.L. & Econ. 1 (1960).

181. 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).

182. See *id.* at 558 ("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.").

Now assume that the law forbids the operation of personal information databases 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 businesses, businesses 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 businesses value the information more than people value their privacy, businesses will purchase the necessary consent.¹⁸³

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 exist; if people value their privacy more, there will be no databases.¹⁸⁴

In fact, comparatively few consumers seem to have taken systematic steps to bar marketers from using their personal data. True, some consumers have acted to curtail the number of solicitations they receive. A number of them have even paid fees to services which purport to reduce or eliminate commercial solicitations.¹⁸⁵ Some consumers have asked to add their names to “opt-out” lists, that is, lists of consumers who do not wish to receive solicitations.¹⁸⁶ The Direct Mailing Association (DMA), a trade association of companies that use direct-mail

183. See Murphy, *supra* note 35, at 2413 (suggesting that merchants could purchase rights from consumers by price differentiation; that is, by charging consumers who withheld permission to use their personal information higher price than consumers who granted permission).

184. Coase's theorem has elicited critical academic discussions, some of which are referred to in Christine Jolls et al., *A Behavioral Approach to Law and Economics*, 50 *Stan. L. Rev.* 1471, 1483 (1998).

185. Perhaps the most prominent of these services is Private Citizen, Inc. A website operated by Consumer Net lists several companies which provide these services. The website is at <<http://consumer.net/optout/consumerfee.asp>> (visited Oct. 6, 1999); see also Scott, *supra* note 71, at 321. Florida has a system in which its residents can pay \$10 to have telemarketers told not to call them. Annual renewals cost five dollars. See Fla. Stat. Ann. § 501.059(3)(a) (West Supp. 1999). Two years after the system's inauguration, 25,000 Floridians had paid the initial fee. See William M. Bulkeley, *Congress's 'Cure' for Junk Calls Faces a Skeptical FCC*, *Wall St. J.*, May 19, 1992, at B6.

186. See Schwartz & Reidenberg, *supra* note 1, at 333 (noting that American Express and Citibank notify cardholders each year that they may opt out); Goodwin, *supra* note 47, at 157.

advertising, maintains a list of 3.3 million consumers who have indicated that they do not wish to receive direct mail.¹⁸⁷ In 1990, a company (then known as New York Telephone) also allowed customers to opt out of a list the company was planning to sell to direct marketers. Of the 6.3 million customers to whom the opt-out offer was made, 800,000 took it.¹⁸⁸

While the total number of consumers who have opted out seems large, the percentage is quite small. Commentators estimate that the proportion of consumers who take advantage of opt-outs is twenty percent or less.¹⁸⁹ This suggests that few consumers are genuinely concerned about solicitations.

B. Are the Surveys Inaccurate?

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

187. See Letter from Michael D. McNeely, Assistant Director, Bureau of Competition, FTC, to Robert L. Sherman, Paul, Hastings, Janofsky & Walter LP (Sept. 9, 1997) <<http://www.ftc.gov/os/1997/9710/dma.htm>> [hereinafter McNeely Letter]. The Direct Marketing Association also maintains a list of consumers who object to telemarketing calls.

188. See Anne W. Branscomb, *Who Owns Information?* 15 (1994). Ultimately, New York Telephone abandoned its plan to sell the list because of consumer opposition. See *Privacy and the NII*, *supra* note 4, at 7 n.26.

189. See Regan, *supra* note 102, at 233. In the fall of 1997, Maryland adopted a system in which drivers could block access to their information. By March 1, 1998, 646,000 (or about 17% of the state's 3.8 million drivers) had opted out. See Chandrasekaran, *supra* note 17, at A1; see also Lukovitz, *supra* note 58, 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."); Laurie Peterson, *The Great Privacy Debate*, ADWEEK—W. Advertising News, Sept. 23, 1991, at 24 ("Studies show that when given the choice, fewer than 10% of consumers will ask to receive no more catalogs."); FTC, *Session Two: Consumer Online Privacy I*, *supra* note 123, at 40 (remarks of Jill A. Lesser, Deputy Director, Law and Public Policy, America Online, Inc.) (reporting that about half a million members of AOL have opted out).

First, the assumption 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, may be faulty. 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 addressed to my wife, but after I made several 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 that sold rather intimate apparel. Once again, I surmised that these companies had purchased my name from companies that sold me children's clothing, I suppose on the assumption that people who buy clothes for children also buy garments for women.¹⁹⁰ I was not so pleased to receive these catalogs. Putting aside the fact that lingerie hardly suits me, I did not need to be reminded about my wife's death by receiving catalogs that should have come to her. The point is, if asked to express my views on privacy and the merits of name-selling, how should I respond? I wanted my name sold to some companies but not to others. I welcomed some solicitations but was saddened by others. My answer 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. However, the surveys are not that narrowly tailored.

190. My guess is that it is more than just an assumption. That is, I suspect that the companies that 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.

Fortunately, my situation is unusual.¹⁹¹ What may not be unusual is that consumers' stated preferences may shift depending on when the questions are posed, what recent experiences the consumer had, and whether the consumer has recently received a wanted or unwanted solicitation. Survey results confirm that consumers do not view all solicitations the same way. The 1996 Equifax-Harris Consumer 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.¹⁹² Only fifteen percent would have their names removed from all lists, while twelve percent would not have their names deleted from any.¹⁹³ Strikingly, among those who indicate that they had experienced invasions of privacy, or think of mail offers as an invasion of privacy or a nuisance, about two-thirds would still keep their names on

191. Others have discussed the pain direct marketers can unwittingly cause. *See, e.g.*, Larson, *supra* note 4, at 11, 83 – 86, 204 – 05 (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 one hundred offers; advice columnist described “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 direct mailer’s ads); Privacy Rights Clearinghouse, *supra* note 71, at 24 (reporting instance where junk mail was still sent to person six years after death; woman who miscarried received baby-related catalogs two years later); R.J. Ignelzi, *Mail and Telejunk*, San Diego Union-Trib., July 4, 1995, at E1 (reporting that woman who had miscarriage received for years solicitations that assumed birth of baby, including birthday cards).

192. *See 1996 Equifax Survey, supra* note 80; *cf. Information Issues: Intellectual Property, Privacy, Integrity, Interoperability, and the Economics of Information*, 48 Fed. Comm. L.J. 5, 41 (1995) [hereinafter *Information Issues*] (remarks of Ellen Kirsh, Vice-President and General Counsel, 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 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.”).

193. Similarly, the 1991 Harris-Equifax Consumer Privacy Survey found that 64% of respondents would choose to have their names removed from some lists, 22% from all lists, and 13% from no lists. *See 1991 Equifax Survey, supra* note 135, at 18 –19.

some direct-mail lists.¹⁹⁴ Consumers also have different reactions to different commercial e-mail offers.¹⁹⁵

The available data probably paint an incomplete picture of consumer preferences, but given the limitations of surveying, it may be impossible to obtain more useful information. Whether this particular problem would underreport or overreport concerns over privacy is hard to determine. On the one hand, surveys may systematically underreport privacy concerns. Consumers who care most about privacy are not likely to answer survey questions precisely because of that concern.¹⁹⁶ On the other hand, surveys may overreport 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.¹⁹⁷ Yet despite these limitations on survey data, it provides the most comprehensive information currently available on consumer attitudes towards privacy.

C. *Why Consumers Might Not Opt Out*

There may be other explanations for the disparity between how surveys suggest consumers should behave and how consumers actually do behave. Consumers face a number of limitations, including informational, logistical, and personal barriers that may impede their ability to opt out of preexisting uses of their personal information.

194. See 1996 Equifax Survey, *supra* note 80.

195. See Westin et al., *supra* note 153, at 23 (“If a procedure were available to block their e-mail addresses from product and service offers, 37% of Internet and online service users who send or receive e-mail would want their addresses blocked from all offers. A large group (50%) would want their address blocked from some offers, and the smallest group (12%) would not want their addresses blocked at all.”) (emphasis in original).

196. See Regan, *supra* note 102, at 49.

197. See *id.*

1. *Consumers Do Not Know About Opt-Outs or How Their Personal Information Is Used*

Some consumers do not take advantage of opt-out lists because they may not know about them. For example, critics say that more consumers would have opted out of the New York telephone company's marketing list if the telephone company had done a better job of informing consumers that they could do so.¹⁹⁸ Similarly, roughly fifty percent of the nation's consumers are said to be unaware of the DMA list— or, in fact, any program that deletes their names from marketing lists.¹⁹⁹ The 1996 Equifax-Harris poll also found that only twenty-nine percent of those who find mail solicitations an invasion of privacy know about name-removal procedures.²⁰⁰

Indeed, few consumers understand how much of their personal information is for sale, although they may have a general idea that there is a trade in personal data and that the specifics about that trade are kept from them. According to one poll, ninety percent of Americans feel that companies do not disclose enough about their list usage.²⁰¹ Yet many consumers remain largely unaware of how businesses use their personal information.²⁰² Even

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

199. See Mary J. Culnan, "How Did they Get My Name?": *An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use*, 17 *MIS Q.* 341, 357 (1993) (finding 78% of participants unaware of procedures to allow mailing list removal); *1996 Equifax Survey*, *supra* note 80 ("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%."); *1991 Equifax Survey*, *supra* note 135, at 18; see also Westin et al., *supra* note 153, at 23 (finding 57% of computer users aware of 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 aware of procedures for removing their e-mail addresses from lists held by companies that send e-mail offers).

200. See *1996 Equifax Survey*, *supra* note 80. One study found that people who were not aware of name-removal procedures were more concerned about privacy. Those people felt, however, that having the opportunity to opt out is less important than did those who were aware of similar procedures. See Culnan, *supra* note 132, at 14–15.

201. See Jones, *supra* note 161, at 139.

202. See Smith, *supra* note 4, at 4 (describing study that finds "consumers tend to be quite uninformed regarding the actual [privacy] policies and practices of industries with which they deal regularly"); Frank V. Cespedes & H. Jeff Smith, *Database Marketing: New Rules for Policy and*

fairly sophisticated consumers may not be fully informed about the use of their personal information. For example, how many readers of this Article were surprised by the available information described in its first pages?²⁰³

The secrecy surrounding how personal consumer information is used limits the potential for consumer action and removes any incentive for companies to restrict their commercial use of such information. Consumers may not know the companies' information policies because those policies are intentionally hidden from them.²⁰⁴ One study reported that when consumers learn of the information practices, "they often become angry and call for legal intervention."²⁰⁵ Paul Schwartz has argued that when consumers believe that their records are protected from

Practice, Sloan Mgmt. 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."); Simson L. Garfinkel, *How Computers Help Target Buyers*, Christian Sci. Monitor, July 25, 1990, at 13 (quoting Bonnie Guiton, Special Advisor for Consumer Affairs to President George 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."); O'Harrow, *supra* note 13, at A1 (quoting Leslie L. Byrne, former director of the Office of Consumer Affairs, as saying: "[M]ost people don't have a clue what's being gathered about them."); *Ticked off at Amex*, USA Today, May 26, 1992, at 10A (describing consumer who assumed that personal data provided to credit card companies and other lenders was protected by business ethics code); Privacy Rights Clearinghouse, *First Annual Report* (visited Oct. 6, 1998) <<http://www.privacyrights.org/ar/annrept.html>> ("Most [consumers] are unaware of the ways in which personal information is . . . used and distributed."); Westin, *Whatever Works*, *supra* note 128 (describing 1997 survey concerning online privacy survey that "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"). 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 *Privacy and Self-Regulation in the Information Age* (visited Oct. 6, 1999) <<http://www.ntia.doc.gov/reports/privacy/selfreg1.htm>>.

203. This lack of awareness 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, *supra* note 4, at 534.

204. See Smith, *supra* note 4, at 4; see also O'Harrow, *supra* note 13, at A1 ("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.").

205. Smith, *supra* note 4, at 4.

disclosure, but businesses know that they are not, a monopoly equilibrium exists.²⁰⁶ Empirical studies seem to confirm that sellers have disproportionate market power when consumers possess imperfect information.²⁰⁷ In such circumstances, sellers cannot be expected to compete on the basis of how much security they provide for information; instead, sellers can be expected to exploit consumer ignorance.²⁰⁸ To put it more bluntly, consumers cannot protect their personal information when they are unaware of how it is being used by others.²⁰⁹

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

207. A number of studies have found that increased comparison shopping by consumers leads to lower market prices. See, e.g., Brian F. Blake et al., *The Impact of Comparative Food Price Information on Consumers and Grocery Retailers: Some Preliminary Findings of a Field Experiment*, 16 J. Consumer Aff. 224 (1982); Kenneth McNeil et al., *Market Discrimination Against the Poor and the Impact of Consumer Disclosure Laws: The Used Car Industry*, 13 L. & Soc'y Rev. 695, 708–09 (1979); J. Edward Russo et al., *An Effective Display of Unit Price Information*, 39 J. Marketing 11 (1975); see also William N. 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, 1111–12 n.96 (1984); Phillip Nelson, *Information and Consumer Behavior*, 78 J. Pol. Econ. 311 (1970); Steve Salop, *Information and Market Structure: Information and Monopolistic Competition*, 66 Am. Econ. Ass'n Rev. 240 (1976) (“[I]f information is costly, each small firm obtains market power, and the equilibrium (if one exists) is characterized by prices above competitive levels.”); Charles Stuart, *Consumer Protection in Markets with Informationally Weak Buyers*, 12 Bell J. Econ. 562 (1981); 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 reduced consumer welfare.”). But see Leon Courville & Warren H. Hausman, *Warranty Scope and Reliability Under Imperfect Information and Alternative Market Structures*, 52 J. Bus. 361, 373 (1979) (stating that “inaccurate information does not necessarily imply poor market results” based on economic model that makes questionable assumption that consumers maximize perceived expected utility).

208. See Schwartz, *supra* note 206, at 49.

209. Cf. Fair Packaging and Labeling Act, Pub. L. No. 89-755, 80 Stat. 1296 (1966) (codified at 15 U.S.C. §§ 1451–1461 (1994)) (“Informed consumers are essential to the fair and efficient functioning of a free market economy.”); FTC Labeling and Advertising of Home Insulation Rule, 44 Fed. Reg. 50,218, 50,223 (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 Bd. of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748, 765 (1976) (stating that “the free flow of commercial information is indispensable” to free enterprise economy).

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."²¹⁰

Consumers seeking to remove their names from lists face other troublesome obstacles. Even if consumers can obtain the information needed to opt out, the cost in time and money of communicating and negotiating with all the relevant information gatherers may be substantial.²¹¹ Anne Wells Branscomb described her experiences:

[A]ttempting 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

210. Enid Nemy & Ron Alexander, *Metropolitan Diary*, N.Y. Times, May 4, 1998, at B2.

211. See Meheroo Jussawalla & Chee-Wah Cheah, *The Calculus of International Communications: A Study in the Political Economy of Transborder Data Flows* 80 (1987); Sandra B. Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 Fed. Comm. L.J. 163, 165 (1995). Swire argues:

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.

Swire, *supra* note 202.

post office box I rented to relieve the overstuffed mailbox at my home address.²¹²

Similar stories abound. One consumer still receives junk mail after having written over 2000 letters seeking deletion from mailing lists.²¹³ 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.²¹⁴ As Joel Reidenberg has written, “This obscured transparency raises transaction costs and allocates them to citizens.”²¹⁵

Special problems in opting out arise in the e-mail context. E-mail addresses cannot be unlisted.²¹⁶ Also, 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 consumers, or even “flame” the customer.²¹⁷ Indeed, this practice is so widespread that some advise consumers unhappy with the promotional e-mail they receive not to seek name

212. Branscomb, *supra* note 188, at 11.

213. See Privacy Rights Clearinghouse, *supra* note 71, at 25; see also G. Bruce Knecht, *Junk-Mail Hater Seeks Profits from Sale of His Name*, Wall St. J., Oct. 13, 1995, at B1 (describing consumer who for years has requested companies to delete his name from their mailing lists but still receives one to seven solicitation letters each day).

214. See Mayer, *supra* note 87.

215. Reidenberg, *supra* note 4, at 533.

216. See Swinson, *supra* note 126, at 23.

217. See Dowd, *supra* note 7, at 110:

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 receives 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.

Id.; see also FTC, *Session Two: Consumer Online Privacy I*, *supra* note 123, at 11 (remarks of Jason Catlett, Chief Executive Officer, Junkbusters Corp.) (stating that some spammers “actually maintain their own pseudo-remove addresses but simply use the results as an additional source of addresses to spam”).

removal.²¹⁸ Consumers who learn that lesson in the e-mail context may carry it over to other contexts, and stop asking that their names be deleted from direct-mail or telemarketing lists.

The DMA has its opt-out lists, but these lists are of limited utility. Many direct marketers eschew the DMA mail list, perhaps because DMA charges for it.²¹⁹ Only a fraction of all companies engaged in direct marketing are members of DMA, and some nonmembers are the ones most likely to misbehave.²²⁰ However, DMA members are said to account for a major percentage of direct-mail solicitations in this country.²²¹ Moreover, registering with DMA will not delete one's name from the mailing lists of political organizations, nonprofits, or local retailers.²²²

DMA members are hardly role models. Reportedly, only about half of the DMA members use the DMA mail preference service to screen their mailings.²²³ Even when companies buy the DMA list, consumers may not be completely satisfied because names often are sold faster than they can be deleted.²²⁴ 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."²²⁵ Moreover, companies

218. See Amy Harmon, *How to, Well, Eat Less Spam*, N.Y. Times, May 7, 1998, at G8.

219. See Allison Fahey, *DMA Speaks to Consumers*, Advertising Age, Apr. 9, 1990, at 63.

220. See Dowd, *supra* note 7, at 110 ("[M]any of the worst offenders are, naturally, not DMA members."); *What Price Privacy?*, *supra* note 30, at 360 ("[S]hady operators are usually not [Direct Marketing A]ssociation members."); Electronic Privacy Info. Ctr., *Comments of the Electronic Privacy Information Center Concerning Children's Privacy* (visited Oct. 6, 1999) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments3/epic3.html>> [hereinafter *EPIC Comments*] (noting that self-proclaimed largest bulk advertising e-mailer in country is not member of DMA).

221. See McNeely Letter, *supra* note 187.

222. See Nora Carrera, *One Man's Junk Is Another's Mail*, Rocky Mountain News, Sept. 25, 1995, at 38A.

223. See Schwartz & Reidenberg, *supra* note 1, at 333 (citing Mary J. Culnan, *Consumer Attitudes Toward Secondary Information Use, Privacy and Name Removal: Implications for Direct Marketing*, Paper Presented at Chicago/Mid-West Direct Marketing Days (Jan. 20, 1993)).

224. See Headden, *supra* note 5, at 42, 48; see also Ignelzi, *supra* note 191 ("It takes between two and six months to have your name and address removed from mailers' lists.").

225. *EPIC Comments*, *supra* note 220; see also Lewyn, *supra* note 115, at 60 (stating that consumers who use DMA list say their names come off some, but not all lists); Beth Givens,

using the DMA opt-out list remain free to maintain and develop profiles on consumers; they are asked only to refrain from soliciting consumers on the list.²²⁶ One frequent commentator on privacy has opined that the DMA list is “meaningless” and “just a public relations effort.”²²⁷

Another significant problem with the DMA list is that placing a name on it is an all-or-nothing decision. Consumers do not have the option of telling DMA which solicitations they prefer and which they disdain.²²⁸ I have chosen not to join 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.²²⁹

Consumers who understand the limitations of the DMA list may rationally choose not to participate in it. 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 telephone would use personal or confidential information in a proper manner—the lowest proportion of any industry inquired.²³⁰ Another survey

Privacy Rights Clearinghouse, *Consumer Privacy 1997—Comments* (visited Oct. 6, 1999) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/sess2com.htm>> (“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.”).

226. See Schwartz & Reidenberg, *supra* note 1, at 333.

227. Lewyn, *supra* note 115, at 60, 61 (quoting Evan Hendricks of Privacy Times).

228. See Direct Mktg. Ass’n, *Fair Information Practices Manual* § 2, at 25 (1994); see also Judith Waldrop, *The Business of Privacy*, Am. Demographics, Oct. 1994, at 46 (quoting Keith Wardell of Buyer’s Choice Media).

229. See *supra* note 192 and accompanying text; see also Waldrop, *The Business of Privacy*, *supra* note 228, at 46 (quoting Keith Wardell of Buyer’s Choice Media as saying: “[W]hat 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.”).

230. See *Equifax-Harris Consumer Privacy Survey 6–7* (1994) [hereinafter *1994 Equifax Survey*]. For companies that offer products or services through the mail, 47% of respondents were

found that many consumers also did not trust companies marketing products on the Internet.²³¹ Indeed, there are reasons to harbor doubts about some marketers, as the preceding paragraphs make clear.

a. The Motivation of Business to Offer Opt-Outs

Firms' motivation for offering opt-out mechanisms affects the ease with which consumers can opt out. Some may offer opt-outs because they are genuinely concerned about the privacy of their customers. Others may offer opt-outs because they view lists that exclude customers who had opted out as more valuable than lists that do not. Some argue that the former lists may command a premium per name because they contain a higher proportion of consumers who are interested in receiving solicitations and, thus, who are more likely to buy.²³² My own experiences suggest that at least some direct marketers are not very concerned with pruning their lists, however. Although my wife has been dead since 1995, we still regularly receive junk mail addressed to her,²³³ and telemarketers still call to speak to her. Companies that genuinely want to eliminate poor sales prospects as a means of making their lists more valuable should probably

not at all confident and 31% were not very confident; the comparable figures for those companies making telephone offers were 54% and 29%; only 5% and 4% were very confident in the use of information by these companies. *See id.*; *see also 1990 Equifax Survey*, *supra* note 45, at 20–21 (reporting that 64% of public had low degree of trust in how companies solicit people by direct mail or telephone collect and use personal information; consumers were more willing to trust every other industry asked about, with the percentage of consumers who had 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. *See Negus*, *supra* note 148, at 64.

231. *See* FTC, *Session Three: Online Privacy*, *supra* note 85, at 157–58 (remarks of Alan Westin, Editor and Publisher, Privacy and American Business; Professor, Columbia University).

232. *See* Knecht, *supra* note 213 (quoting Eli Noam, Professor of Finance and Economics at Columbia University, 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.").

233. This is not unusual. *See* Privacy Rights Clearinghouse, *supra* note 71, at 24 (reporting that person who died six years ago still receives direct mail ads); Widows & Widowers Newsl., Sept. 25, 1998 (on file with author) (reporting that deceased people still receiving mailings).

start with those who have died, yet at least some do not.²³⁴

Other companies may offer customers an opportunity to opt out because they believe it preserves customer good will.²³⁵ Consumers who are concerned about privacy might prefer a company that respected their wishes. Even consumers who do not value privacy might favor such a company for respecting consumer concerns. As a result, these companies may consider allowing opt-outs as a marketing advantage.

A handful of companies have chosen to compensate consumers for their personal information, or to market themselves on the basis of privacy.²³⁶ 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.²³⁷ 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.²³⁸ In the long-distance telephone market, one company has advertised that it will

234. My wife's death occasioned an obituary in the New York Times on August 10, 1995. If they wish to, marketers could keep up with obituaries just as they keep up with birth announcements. For a 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 (1994) (reporting that diaper manufacturer knows names of over 75% of expectant mothers in United States; obtained information from doctors, hospitals, and childbirth trainers). See generally Larson, *supra* note 4.

235. See Ann Cavoukian & Don Tapscott, *Who Knows: 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."); Reidenberg, *supra* note 4, at 533 ("[B]usiness is beginning to grasp that better standards for fair information practice can be a competitive advantage and will be necessary for business survival.").

236. At least two businesses have voluntarily decided to use an opt-in system: the Microsoft Network, commonly known as MSN, and USA Today. See Cavoukian & Tapscott, *supra* note 235, at 69–70, 94–95.

237. See Scott, *supra* note 71, at 322.

238. See Munro, *supra* note 82; 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 months to receive coupons in return for personal information); cf. *infra* note 368 and accompanying text.

not use customer calling records to identify and solicit others, while another company apparently does just that.²³⁹ However, these stories are the exceptions.²⁴⁰

For the most part, companies have chosen not to offer incentives to surrender privacy, and not to compete by offering consumers more privacy.²⁴¹ 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 with each other on privacy because "it falls into the category of 'negative' information about a company."²⁴² She argues that businesses have little incentive to make investments to protect the security of their information systems and are unlikely to advertise that their practices

239. See Swire, *supra* note 202. Similarly, a credit card company now includes in its solicitations a statement that it will not sell customer names to other companies. See John N. Frank, *The Brouhaha over Privacy*, Credit Card Mgmt., May 1996, at 32, 33; see also Knecht, *supra* note 213 (reporting that American Express, Citicorp, and Dow Jones & Co. allow consumers to opt out because of companies' desire not to upset their customers). Richard Murphy has collected two examples of companies which conspicuously tell consumers that they do not sell their mailing lists. One is Radio Shack, which posts signs to that effect near its cash registers. See Murphy, *supra* note 35, at 2413–14 nn.165 & 166.

240. Cf. Kang, *supra* note 84, at 1248 ("For numerous reasons . . . individuals and information collectors do not generally negotiate and conclude express privacy contracts.").

241. 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 *Privacy and the NH*, *supra* note 4, at 20. That problem may be solvable by regulation, however, just as other problems created by the necessarily monopolistic nature of some service providers are solved.

242. Jones, *supra* note 161, at 139; see also Kang, *supra* note 84, at 1255 ("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."); Murphy, *supra* note 35, at 2414 ("Raising the privacy issue may evoke negative reactions in consumers who otherwise would not have thought about the issue.").

are risk-free.²⁴³ In fact, sellers may choose not to advertise product attributes for a variety of reasons.²⁴⁴

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.²⁴⁵ Indeed, the DMA—an organization that recently began requiring its members to comply with its opt-out system—has lobbied extensively against privacy legislation and started its opt-out lists in part to avoid such legislation.²⁴⁶ 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 suggested or mandated, in one form or another, adoption of certain fair information practices.²⁴⁷ These countries have agreed that fair information practices should include, among other

243. Mary 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 examples 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. See Jones, *supra* note 242, at 139.

244. See, e.g., E. Patrick McGuire, *Industrial Product Warranties: Policies and Practices* 10 (1980) (describing study of 369 manufacturers that 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) (reporting that car dealers do not disclose markups even though different dealers use different markups and consumers pay third parties for markup information).

245. 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).

246. See Schwartz & Reidenberg, *supra* note 1, at 309 n.5, 332; Foxman & Kilcoyne, *supra* note 25, at 113; Evan Hendricks, *DMA Will Raise \$2.6 Million War Chest to Fight U.S. & State Privacy Measures*, Privacy Times, Apr. 22, 1992, at 2. For a discussion of DMA's motivation in starting opt-out lists, see Alan F. Westin & Michael A. Baker, *Databanks in a Free Society: Computers, Record-Keeping and Privacy* 166 (1972).

247. See, e.g., Organization for Econ. Cooperation & Dev., *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1981); Canadian Standards Ass'n, *Model Code for the Protection of Personal Information* (1996); Privacy Protection Study Comm'n, *Personal Privacy in an Information Society* (1977); *Privacy and the National Information Infrastructure*, *supra* note 55; U.S. Dep't of Health, Educ. & Welfare, *Records, Computers and the Rights of Citizens* (1973).

things, that businesses give consumers notice before collecting information from them, and that consumers be given options as to how such information will be used.²⁴⁸

b. The Impact of Transaction Costs on Opting Out

Companies may not be eager to offer opt-outs because they may rationally conclude that they will incur costs when consumers opt out, while receiving few offsetting benefits. When consumers exercise the option of having their names deleted, mailing lists shrink and presumably become less valuable.²⁴⁹ Moreover, companies will incur transaction costs in notifying consumers of the existence of the opt-out option and in responding to consumers who opt out.²⁵⁰

Companies may respond to these costs by charging consumers for opting out. This charge could be imposed in a number of ways, including offering a discount to consumers who do not opt out.²⁵¹ A downside to this approach, however, is that it might generate consumer resentment, conceivably causing some consumers who might otherwise have purchased a company's product to walk away from the transaction altogether. Perhaps the fear of this negative consequence is why so few sellers offer a

248. See FTC, *Privacy Online*, *supra* note 39, at 7, 8.

249. However, 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, as well as a function of how many consumers actually opt out, how many do not opt out, and the costs of administering the opt-out program. See *supra* note 232 and accompanying text.

250. See, e.g., FTC, *Session Two: Consumer Online Privacy II*, *supra* note 144, at 223 (remarks of Martin Nisenholtz, President, New York Times Electronic Media Co. and Coalition for Advertising Supported Information and Entertainment) (noting that when subscribers ask Times to implement its web site privacy policy, Times incurs costs of around \$5 per person to do so).

251. See D'Amato, *supra* note 103, at 501 (suggesting that magazine publishers could institute two-tiered subscription price: those who do not want their names sold would pay more); see also Foxman & Kilcoyne, *supra* note 25, at 109 ("One possible solution to this particular ethical 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.").

differential pricing scheme. Thus, in the end, sellers who offer opt-out systems will likely absorb the costs of doing so themselves.

Because of these added costs, companies might decide that while they must offer an opt-out plan, they do not want consumers to take advantage of it.²⁵² Such companies might understandably provide opt-out mechanisms without making them easy to use.²⁵³ To put it another way, companies that offer opt-outs have an incentive to increase the transaction costs incurred by consumers who opt out. This explains why a market in privacy and consumer information consistent with Coase's theorem has not emerged. As Coase himself recognized, the Coase theorem is a prisoner of its underlying assumption that no transaction costs exist. That assumption does not apply here.

Avery Katz has identified two types of transaction costs: costs of implementation and costs of strategic behavior.²⁵⁴ 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."²⁵⁵ In an opt-out context,

252. Cf. Karl Dentino, *Taking Privacy into Our Own Hands*, Direct Marketing, Sept. 1994, at 38, 40:

Offer opt-out, but carefully. . . . [O]pt-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 thoughtfully consider direct mail offers.

253. Cf. William C. 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).

254. 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).

255. *Id.*

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."²⁵⁶ 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.

It is unclear whether consumers will respond to the increased transactions costs by forgoing purchases. Some consumers seem to have done just that when it comes to the Internet. Nevertheless, many consumers buy goods and services through other media that permit the collection of their personal information. Again, some consumers may not know of the uses to which their information is being put. Yet, even a knowledgeable consumer may decide to 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 he or she values the product more than the costs involved in obtaining it. The costs of obtaining the product include the purchase price plus the lesser of the cost of opting out or the value of the lost privacy. The idea may be expressed as follows: where V_P is the value of the purchase to the consumer, P is the purchase 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 $V_P > P + (\text{lesser of } C_{OO} \text{ and } V_{LP})$.

The reason the consumer should focus on the lesser of the cost of opting out and the value 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 simply endure

256. *Id.* at 226.

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.

If businesses inflate the cost to consumers of opting out, some consumers should respond by declining to buy, and businesses will lose sales. It therefore seems counterintuitive that businesses will inflate the costs to their customers, especially when the added costs will not generally represent revenues received by the businesses. Recall, however, that a number of businesses generate more revenue from sales of mailing lists than from the products they sell. Such businesses have an incentive to inflate the costs to consumers of protecting their privacy until the loss of profit from lost product sales exceeds the profits 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 transaction costs may be small.

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

(2) consumer 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 privacy into account in deciding whether to make the purchase. Presumably, some nescient consumers will end up purchasing under equation (2), when they would not otherwise have bought under equation (1). Such purchases reduce society's net welfare, but 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. This potential double gain may be another reason why sellers do not, with some exceptions, publicize their information practices.

Companies can increase consumers' transaction costs in opting out in a number of ways. A brochure titled "Privacy Notice," which my local cable company included with its bill, provides an example.²⁵⁷ This Privacy Notice discussed, among other things, how cable subscribers could write to the company to ask that the company not sell their names and other information to third parties. There are at least four reasons why this particular notice may not be effective in eliciting a response from consumers troubled by the sale of their names to others.

First, the Privacy Notice may be obscured by other information included in the mailing. The Privacy Notice arrived with a bill and the monthly Pay-Per-View listings, both likely to be of greater interest to consumers than other printed inserts. Social scientists have found that consumers are more likely to focus on "vivid" information such as the Pay-Per-View listings, which were written in considerably more exciting prose and included color photographs, than on duller information.²⁵⁸ Similarly, consumers focus more on pictures—again, like those in the Pay-Per-View listings—than on text.²⁵⁹

The second reason why consumers may not respond to the Privacy Notice is its length. The brochure is four pages

257. Under the Cable Communications Policy Act of 1984, as amended by the Cable Television Consumer Protection and Competition Act of 1992, 47 U.S.C. §§ 521–558 (1994), 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).

258. See Richard E. Nisbet & Lee Ross, *Human Inference: Strategies and Shortcomings of Social Judgment* 45 (1980); Jonathan Shedler & Melvin Manis, *Can the Availability Heuristic Explain Vividness Effects?*, 51 J. Personality & Soc. Psychol. 26 (1986); Margaret G. Wilson et al., *Information Competition and Vividness Effects in On-Line Judgments*, 44 Organizational Behav. & Hum. Decision Processes 132 (1989). A story makes the point even more clearly: Some years ago, federal regulation 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. See Alan Schwartz & Robert E. Scott, *Commercial Transactions: Principles and Policies* 1142 (2d ed. 1991).

259. See Nisbet & Ross, *supra* note 258, at 51; 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).

long and contains 17 paragraphs, 36 sentences, and 1062 words. While some reports are to the contrary, many studies have now demonstrated the existence of “information overload,” meaning that overloaded consumers either do not make optimal decisions or overlook relevant information.²⁶⁰ 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.²⁶¹ Consequently, some consumers may be deterred from reading the Privacy Notice, 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 description of 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 companies state only that they may make offers they “think would be of interest to you.”²⁶² While some companies may have made this type of limited disclosure in good faith, commentators have suggested that “the vagueness intentionally avoids giving individuals knowledge of actual practices.”²⁶³ Regardless of a company’s intent, a limited or vague disclosure is unlikely to assist consumers in determining whether to opt out.

260. See, e.g., John C. Bergstrom & John R. Stoll, *An Analysis of Information Overload with Implications for Survey Design Research*, 12 *Leisure Sci.* 265 (1990); Kevin L. Keller & Richard Staelin, *Effects of Quality and Quantity of Information of Decision Effectiveness*, 14 *J. Consumer Res.* 200, 211 (1987); Naresh K. Malhotra, *Information Load and Consumer Decision Making*, 8 *J. Consumer Res.* 419 (1982). For a critical analysis of the Keller & Staelin study, 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 Melvin Eisenberg, *Text Anxiety*, 59 *S. Cal. L. Rev.* 305 (1986); David M. Grether et al., *The Irrelevance of Information Overload: An Analysis of Search and Disclosure*, 59 *S. Cal. L. Rev.* 277 (1986); 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).

261. See, e.g., Katz, *supra* note 254, at 273.

262. Schwartz & Reidenberg, *supra* note 1, at 280.

263. *Id.*

A third reason why the Privacy Notice may not be effective stems from its prose. Notwithstanding the Plain Language Law in my home state,²⁶⁴ computer analysis of the text found it extremely difficult, requiring more than a college education for comprehension.²⁶⁵ By comparison, a similar analysis of this Article found that it required a lower reading level than that of the Privacy Notice.

Fourth, the Privacy Notice may be ineffective because it does not provide an easy or convenient mechanism for opting out. For example, the Privacy Notice invites consumers who object to the sale of their personal information to write to the cable company in a separate letter. By contrast, cable subscribers desiring to add a new premium channel can do so over the telephone, speaking either to a person or tapping buttons on their telephone, depending on their preference. The more difficult the opt-out process, the less likely consumers are to avail themselves of it.²⁶⁶

My cable company is hardly unique in the presentation of its opt-out policy. In 1996, Congress amended the Fair Credit Reporting Act to provide that information otherwise covered by the statute could be shared among commonly owned businesses "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

264. See N.Y. Gen. Oblg. Law § 5-702 (McKinney 1989) (requiring consumer agreements to be "[w]ritten in a clear and coherent manner using words with common and every day meanings"). Arguably, the Plain Language Law does not apply to the Privacy Notice because the statute governs only written agreements, and the Notice may not be an agreement. Still, properly construed, the Plain Language Law should have some persuasive effect on virtually all documents for consumers.

265. The Flesch Reading Ease score was 28; the scale ranges from zero (hardest) to 100 (a fourth grade level). Scores between zero and 30 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.

266. Cf. Charles D. Raab et al., *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) ("[S]ome companies that offer an opt-out require consumers to send a letter separately from an order and to a different address.").

be communicated among such persons.”²⁶⁷ 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.”²⁶⁸ Then-Acting Comptroller of the Currency Julie Williams commented, “Most bank customers can’t ever recall seeing something like this.”²⁶⁹ She further observed:

[I]t 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.²⁷⁰

Not surprisingly, banks are not the only companies that provide opt-out notices in small print.²⁷¹ Similar

267. 15 U.S.C.A. § 1681a(d)(2)(A)(iii) (West Supp. 1999). 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. See Leslie Wayne, *Privacy Matters: When Bigger Banks Aren’t Better*, N.Y. Times, Oct. 11, 1998, § 4 at 4.

268. Wayne, *supra* note 267, §4 at 4.

269. *Id.*

270. Office of the Comptroller of the Currency, U.S. Treasury Dep’t, *Remarks by Julie L. Williams, Acting Comptroller of the Currency, Before the Banking Roundtable Lawyers Council* (May 8, 1998) <<http://www.occ.treas.gov/ftp/release/98%2D50a.txt>>; see also Office of the Comptroller of the Currency, U.S. Treasury Dep’t, *Remarks by Julie L. Williams, Acting Comptroller of the Currency, Before the Consumer Bankers Association* (Oct. 26, 1998) <<http://www.occ.treas.gov/ftp/release/98-109a.txt>>.

271. See Larson, *supra* note 4, at 90; David J. Klein, Note, *Keeping Business out of the Bedroom: Protecting Personal Privacy Interests from the Retail World*, 15 J. Marshall J. Computer & Info. L. 391, 398 (1997) (“List creators generally place [opt-out provisions] in the fine print with

complaints have been made about online disclosures of privacy policies.²⁷² Other examples are not hard to find. In 1995, TRW (now Experian) published a booklet entitled “Twelve Common Questions about Consumer Credit and Direct Marketing.” It is not until the twelfth—and last—question, beginning on page sixteen, that the booklet addresses how to remove names from TRW’s marketing list. An earlier question, for example, inquires, “How does a credit bureau help me?”²⁷³

A merchant’s motive becomes questionable when the merchant provides subscribers with a lengthy, dull, and difficult-to-read statement of their rights and requires subscribers wishing to opt out to communicate their intent in a separate writing.²⁷⁴ The merchant’s motive is particularly suspect if other solicitations are provided in exciting, brief language with pictures and if the advertised goods or services can be purchased over the telephone. 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)

other boilerplate terms of the contracts; thus the clause is not readily apparent to most consumers.”) (footnotes omitted); Lewyn, *supra* note 115, at 60, 61; Privacy Rights Clearinghouse, *supra* note 71, at 27.

272. See FTC, *Session Three: Consumer Online Privacy*, *supra* note 85, at 218. Mary E. Fise, General Counsel of Consumer Federation of America, remarked:

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.

Id.

273. More recently my cable company republished its privacy notice in a brochure titled “Your Cable Equipment and Services.” The brochure runs 20 pages, and the privacy notice—the last item in the booklet—begins on page 17 and concludes on page 20. The brochure arrived in an envelope with the 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.”

274. See also Waldrop, *supra* note 228, at 48 (quoting Georgetown University Professor Mary Culnan’s statement, made at 1994 DMA meeting, that “fifty percent of catalogers don’t give their customers a convenient way to remove their names from the company’s list”).

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.”²⁷⁵ 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 messages 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 [the toll free number] or mark here.” The form provides an oval which members can mark and return to the ABA along with their answers to other inquiries. In comparing ABA’s census form with the cable company’s Privacy Notice, it may be relevant that the ABA is a nonprofit organization operated at least in part for the benefit of its members.²⁷⁶

An opt-out system like the one used by my cable company is unlikely to reflect consumer preferences accurately. Under such a system, numerous people who do not wish to receive solicitations receive them, and personal information is sold about many people who would prefer it not to be sold. The system cannot reflect true consumer preferences because the availability of an opt-out mechanism is obscured and the mechanism itself cannot easily be used. As a result, as long as marketers

275. George S. Day, *Assessing the Effects of Information Disclosure Requirements*, J. Marketing, Apr. 1976, at 42, 47; see also Eskridge, *supra* note 207, at 1163 – 64.

276. Although 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—the product of an agreement between American Express 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 reproduced at *American Express/New York Attorney General Agreement Announced*, PR Newswire, May 13, 1992.

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 the failure of consumers to opt out as often as their survey answers might suggest is the consumers themselves. Extensive literature on consumer complaint behavior makes clear that many consumers who are distressed by merchant conduct cannot bring themselves to tell the merchant about it.²⁷⁷ This inability to communicate might translate into failure by consumers to add their names to opt-out lists. The appropriate response to this behavior may be 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 do not act are making a statement that their privacy is not worth very much to them. If privacy is not worth very much to most consumers, then perhaps society would be better off focusing on other concerns that matter more to consumers.

In reality, however, consumers act inconsistently with regard to their preferences. Why do consumers do that? E. Scott Maynes has argued that consumers suffer from handicaps when dealing with business, handicaps that contribute to asymmetries in the consumer-business relationship.²⁷⁸ The first handicap, according to Maynes, is that a person's interest as a consumer is subordinate to his or her job, at least until retirement.²⁷⁹ Consequently, "many consumers cannot find the time to manage

277. 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. See 6 J. Consumer Satisfaction, Dissatisfaction & Complaining Behav. 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'y Rev. 701, 712 (1977) (reporting that only 30.7% of consumers perceiving problems voice complaints).

278. See E. Scott Maynes, *Consumer Problems in Market Economies*, in *Encyclopedia of the Consumer Movement* 158–59 (Stephen Brobeck ed., 1997).

279. See *id.* at 158.

effectively consumption that has grown more complex and dynamic.”²⁸⁰

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 a consumer, by contrast, one’s interest is spread thinly across thousands of transactions and the management of hundreds of possessions.”²⁸¹ 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.

c. The Analogy to “Negative Option Billing”

The opt-out situation may be compared to what is sometimes called “negative-option billing.” Negative-option billing is often used by book and music clubs. Typically, from time to time, members of the club receive a brochure describing the club’s offerings. If members do not respond by a particular date, the items are automatically sent to them. Members who do not wish to receive the goods must mail a notice to that effect to the club.²⁸² In this way, companies make a consumer’s failure to act an acceptance of the product.

As one consumer attorney has written, “As 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.”²⁸³ The

280. *Id.* at 163; 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.”).

281. Maynes, *supra* note 278, at 158–59.

282. Negative-option purchases are regulated by the FTC. See 16 C.F.R. § 425.1 (1999).

283. Bruce A. Craig, *Negative-Option Billing: Understanding the Stealth Scams of the ‘90s*, 7 Loy. Consumer L. Rep. 5, 6 (1994); see also Meg Cox, *For the Nation’s Troubled Book Clubs*, *Main*

empirical evidence available shows rather emphatically that negative options make a substantial difference to consumer behavior. For example, 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 forty-four percent 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 thirty-six percent of the consumers.²⁸⁴

Similar results have shown up in the cable television industry. In Canada, cable television companies found that when new channels were offered in normal ways in Nova Scotia, only twenty-five percent of customers subscribed, but when made available through negative options, as they were in the rest of Canada, sixty to seventy percent subscribed.²⁸⁵ In other words, for many cable customers, the key factor in making the purchasing decision is not the cost or content of the programming, but whether they have to affirmatively subscribe or unsubscribe.

Merchandisers have acknowledged that consumers buy more readily when items are sold through negative options.

Selection of This Year Is Change, Wall St. J., July 24, 1992, at B1 (“[R]eceiving main selections [members] don’t want but have forgotten to cancel is one of the most annoying aspects of book clubs.”).

284. The FCC examined 50 cases of positive-option offers and 22 cases of negative-option offers. See FCC, *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 UCLA L. Rev. 1315, 1330–31 (1995); see also Owen R. Phillips, *Negative Option Contracts and Consumer Switching Costs*, 60 S. Econ. J. 304, 305 (1993) (“[U]nder 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.”).

285. See William Walker, *NDP Set to Ban Negative Billing and Cable Subscribers Could Get a Break*, Toronto Star, Feb. 24, 1995, at A3; see also Ian Austen, *Rogers Demands Dismantling of Stentor*, Calgary Herald, Jan. 27, 1995, at D14 (reporting cable company official predicted lower number of subscribers unless negative option used); Robert Brehl, *Rogers TV Woes Don’t Hit Shares*, Toronto Star, Jan. 7, 1995, at C2 (reporting that cable company forecasts “dramatically” fewer subscribers if negative option not used).

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 eighty percent to fifty percent.²⁸⁶ Similarly, when the FTC took testimony on negative-option selling, several sellers acknowledged that fewer subscribers would purchase the goods offered if buying them required affirmative action.²⁸⁷

No one suggests that consumers would respond to all negative-option offerings equally. To take a fanciful example, if a business supplies a service priced at \$20,000 unless the consumer returns an enclosed form, in which case the same service would cost \$10, surely every consumer who desires the service would send in the form. Privacy, however, seems less like the \$20,000 service 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 do not notice that they are making the purchase.²⁸⁸ 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

286. See Kathy Clayton, *Subs to TCI: We Want Our \$1 Encore*, Cable World, July 1, 1991, at 1, 20.

287. See 38 Fed. Reg. 4896, 4902 (1973) (regarding use of negative-option plans by sellers in commerce). The FTC cautioned, 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 system." *Id.* It 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.

Id. 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. See *id.* at 4902-03.

288. See Craig, *supra* note 283, at 8.

to the charge.”²⁸⁹ Obviously, a system in which people make purchases that do not reflect their preferences is inefficient.

The analogy to negative options seems clear: if the default rule is that inaction equals loss of privacy, then consumers are likely to surrender their privacy in a way that does not reflect their actual preferences. To be sure, the current default rule does not affect consumers who are troubled enough about the loss of privacy to have taken affirmative action to protect their privacy. Nor does it make a difference to those who do not care about privacy. The default rule does matter, however, for those consumers who do not want to give up their privacy, but who will not act to change the default to one that more closely reflects their preferences. For many consumers, the default rule matters a great deal because it affects choices.

IV. FIXING THE PROBLEM

Making commercial practices more consistent with consumer preferences requires that consumers be better informed, unnecessary transaction costs be eliminated, and barriers to consumers’ acting in accord with their preferences be minimized. As discussed above, we do not have that today: consumers often find it difficult to opt out, and it appears that businesses have the incentive and the power to make it that way. Options do exist, however, for improving the system.

A. *A Voluntary System*

One possibility is for businesses to move voluntarily to an opt-out system, free of government regulation— except perhaps government enforcement of broken promises.

289. *Id.* at 9.

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.

Id.

Surveys have generally shown that consumers prefer voluntary privacy policies to legislation (although consumers would support changes in existing law if companies fail to adopt appropriate privacy policies).²⁹⁰ There are reasons for believing that voluntary participation in such a voluntary system may become a reality. Many trade guidelines already call upon businesses to provide notice of their information policies and to allow consumers to opt out.²⁹¹ Since July 1999, DMA members have had to notify consumers of their information practices and permit consumers to opt out.²⁹² The DMA is also developing a list of consumers who do not wish to receive unsolicited commercial e-mail, similar to its existing lists of those who object to mail and telephone solicitations.²⁹³

Progress has also been made in preserving privacy on the Internet. For now, the FTC is content with seeking self-regulation of the Internet insofar as adults are

290. See Westin & Maurici, *supra* note 128, at 34 (reporting 79% of computer users, 80% of Internet users, and 76% of Internet purchasers prefer privacy self-regulation to government regulation of Internet, and feel that government should regulate only if self-regulation fails); Westin, *Whatever Works*, *supra* note 128 (finding that 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).

291. See, e.g., Banking Indus. Tech. Secretariat, The Bankers Roundtable, *Privacy Principles Implementation Plan 2*; Direct Mktg. Ass'n, Inc., *Direct Marketing Association Guidelines for Ethical Business Practice* 13; Interactive Serv. Ass'n, *Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators*; Letter from Donald D. Kummerfeld, President, Magazine Publishers of Am., to Donald Clark, Secretary, FTC (Mar. 31, 1998); Smart Card Forum, *Guide to Responsible Consumer Information Practices*; Letter from Kerry C. Stackpole, President & Chief Executive Officer, Electronic Messaging Ass'n, to Robert Pitofsky, Chairman, FTC (Mar. 31, 1998). These documents are reproduced in FTC, *Privacy Online*, *supra* note 39. See also Evan Hendricks, *Advertisers Unveil 'Goals' for Electronic Privacy*, *Privacy Times*, Feb. 15, 1996, at 3; Evan Hendricks, *Bankers Issue 'Best Practices' Guidelines for Customer Data*, *Privacy Times*, Dec. 17, 1996, at 4 (discussing Consumer Bankers Association guidelines).

292. See Rajiv Chandrasekaran, *Direct Marketing Group Adopts New Guidelines; Rules Are an Attempt to Avoid Intervention by Federal Regulators*, *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 consumers with an opportunity to opt out. See *Privacy and the NII*, *supra* note 4, at 23–24.

293. See *Cramming and Spamming Hearings*, *supra* note 68 (testimony of Jerry Cerasale, Senior Vice-President, Direct Marketing Association).

concerned.²⁹⁴ Recently, a number of corporations and associations, under the aegis of the online Privacy Alliance, adopted guidelines for online privacy policies.²⁹⁵ One third-party oversight privacy program, TRUSTe, claims that one-quarter of the time spent on the Internet is spent on sites licensed by TRUSTe.²⁹⁶ The Better Business Bureau has also established a self-regulatory program.²⁹⁷ A 1999 Georgetown University survey found that nearly two-thirds of the sites in its sample contained at least one privacy disclosure.²⁹⁸ Adding to the pressure, IBM and Microsoft have announced that they will no longer advertise on web sites that do not post privacy policies.²⁹⁹

The information industry itself appears amenable to voluntary approaches. 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

294. See FTC, *Self-Regulation & Privacy Online: A Report to Congress* (1999).

295. See Jeri Clausing, *Group Proposes Voluntary Guidelines for Internet Privacy*, N.Y. Times, July 21, 1998, at D4; Robert O'Harrow, Jr., *Firms Prepare Plan for Protecting Privacy on Internet*, Wash. Post, June 20, 1998, at D3. The Alliance's website is at <<http://www.privacyalliance.org>>.

296. See *Industry Hopes Seal-of-Approval Programs Will Meet Privacy Self-Regulation Challenge*, 67 U.S.L.W. 2396, 2397 (Jan. 12, 1999) [hereinafter *Seal-of-Approval Programs*] (reporting 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 <<http://www.truste.org>>. TRUSTe was recently criticized by privacy advocates for failing to audit Microsoft, one of its biggest donors, after Microsoft was accused of collecting consumer data surreptitiously. TRUSTe did scold Microsoft. See Jeri Clausing, *On-Line Privacy Group Decides Not to Pursue Microsoft Case*, N.Y. Times, Mar. 23, 1999, at C5.

297. See *Seal-of-Approval Programs*, *supra* note 296, at 2397. To earn a BBB seal, participants must disclose to visitors to the site, among other things, the type of information collected, the methods available to consumers to correct erroneous information, and whether the information is merged with other information obtained from third parties. The Better Business Bureau's program web site is at <<http://www.bbbonline.org>>.

298. See Culnan, *supra* note 39, at 7.

299. See Online Privacy Alliance, *Senate Judiciary Committee Holds Internet Privacy Hearing* (visited Oct. 6, 1999) <http://www.privacyalliance.org/news/04211999_test/ibm_written.shtml> (statement of Dr. Irving Wladawsky-Berger, General Manager, Internet Section, IBM Corp.).

subscribers,” like investigators, insurers, and lawyers.³⁰⁰ While this voluntary step appears promising, it occurred only after businesses faced involuntary government regulation, and it still permits access to the information by some who arguably should not have it.

Nevertheless, pessimism about the willingness of the information industry to adopt a consumer consent system seems more justified, given the limited efforts taken to date to protect consumer privacy and their questionable effectiveness. Critics of the information industry complain that self-regulation has not been effective.³⁰¹ The reported failure of half of DMA’s membership to use DMA’s mail preference service lends credence to such claims.³⁰²

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

301. See, e.g., S. 2326, *the Children’s Online Privacy Protection Act of 1998: Hearings on S. 2326 Before the Subcomm. on Communications of the Senate Comm. on Commerce, Science, & Transp.*, 105th Cong. (1998) (testimony of Kathryn Montgomery, President, Center for Media Education) (“[T]he absence of a certifying seal is too subtle a means of educating Internet users.”); Schwartz & Reidenberg, *supra* note 1, at 217; Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. Rev. 847, 874 (1998) (“[T]he presence of great diversity in [the online] industry makes universal participation [by marketers] unlikely.”); Culnan, *Self-Regulation on the Electronic Frontier*, *supra* note 178 (arguing that self-regulation has been ineffective because rules have not been applied equally to all firms within industry and because data compilers do not have direct contact with consumers); FTC, *Session One: Database Study*, *supra* note 21, at 188 (remarks of Beth Givens, Project Director, Privacy Rights Clearinghouse); *id.* at 319 (remarks of Evan Hendricks, Editor and Publisher, *Privacy Times*) (“There has been a long history of failure of self-regulation meeting privacy concerns in this country going back to . . . [the] late 1970s.”); FTC, *Session Two: Consumer Online Privacy II*, *supra* note 144, at 152 (remarks of Russ Smith, Publisher, Consumer.Net); *id.* at 175 (remarks of Jean Ann Fox, Director of Consumer Protection, Consumer Federation of America; Vice-President, Consumers Union) (“[S]elf-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, 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.”); Pasnik & Fise, *supra* note 42. *But see* Robert J. Posch, Jr., *Keep the Privacy Debate in Context*, *Direct Marketing*, May 1, 1997, at 1 (stating that 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* 3 (1998) (“[S]elf-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.”).

302. See *supra* note 223 and accompanying text.

Commentators have charged that the DMA Code of Fair Information Practices "is not systematically honored by companies engaged in direct marketing activities."³⁰³ Nor does the DMA maintain data on compliance with its Code.³⁰⁴ 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.³⁰⁵ Members of the DMA's Privacy Task Force themselves are said to ignore DMA guidelines;³⁰⁶ in fact, a representative of the company which entered into the \$400,000 settlement chaired the DMA Privacy Task Force.³⁰⁷ 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.

With respect to Internet sites,³⁰⁸ 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 requirements.³⁰⁹ Even a DMA official has acknowledged that "we clearly still have a way to go."³¹⁰ The 1999 Georgetown survey, while concluding

303. Schwartz & Reidenberg, *supra* note 1, at 217.

304. *See id.*

305. *See id.* at 338-39; *see also* FTC, *Session One: Database Study*, *supra* note 21, at 288 (remarks of Robert Biggerstaff, who has 30 years of experience in the database field) ("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* Direct Marketing Association, Inc., *Supplemental Comments of the Direct Marketing Association, Inc.* (July 6, 1997), in *Public Workshop on Consumer Information Privacy* <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/dma027a.htm>> (stating that DMA will refer non-complying members to DMA Committee on Ethical Business Practice which publishes compilation of cases it reviews).

306. *See* Schwartz & Reidenberg, *supra* note 1, at 309.

307. *See id.* at 338-39.

308. For a discussion of the relative merits of self-regulation and government regulation in the privacy context, see Swire, *supra* note 202.

309. *See* Electronic Privacy Info. Ctr., *Surfer Beware II: Notice Is Not Enough* (visited Oct. 6, 1999) <<http://www.epic.org/reports/surfer-beware2.html>>.

310. *Id.* (quoting Patricia Faley, Vice-President of Consumer Affairs, Direct Marketing Association, Inc.).

that many sites now contain privacy disclosures, also found that only 14.8% of the sites in its sample contained all five elements of fair information practices, as they are defined by the survey.³¹¹

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. One of its services, "Checkmate," allows customers to investigate the people they are dating.³¹² Moreover, one member of the online Privacy Alliance has already been accused by the FTC of misrepresenting how it uses collected data. The matter terminated in a settlement in which the company did not admit wrongdoing.³¹³

Even more troubling is the failure of the information industry to comply with existing laws, let alone nonbinding industry guidelines. For example, when a trade magazine wrote to forty-eight telemarketers requesting copies of their "Do Not Call" policies, which telemarketers are required to provide upon request,³¹⁴ only seventeen had responded after three months.³¹⁵ Accordingly, if the information industry as a whole is to adopt a consumer-consent regime, government intervention is likely to be needed.

B. A Mandated Opt-Out System

One solution requiring government intervention would be to establish mechanisms to inform consumers about the choices available to them and to eliminate unnecessary

311. See Culnan, *supra* note 39, at 8.

312. See Evan Hendricks, *Look-Up Service Spokesman Doubts Efficacy of FTC-Industry Agreement*, Privacy Times, Mar. 6, 1998, at 1, 2.

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

314. See 47 C.F.R. § 64.1200(e)(2) (1999).

315. See Evan Hendricks, *Telemarketers Accused of Ignoring Junk Phone Law*, Privacy Times, June 12, 1998, at 5-6; see also William M. Bulkeley, *Congress's Cure for Junk Calls Turns into Skepticism at the FCC*, Wall St. J., May 19, 1992, at B6 (reporting that consumers on Florida's "don't call" list who continue to receive unsolicited calls took their names off list).

transaction costs. This solution would still preserve the default rule that if consumers do not act, businesses can trade their information, while improving the ability of consumers to opt out. For example, such a rule could specify the content of consumer notices so that such notices would be more attractive and comprehensible. A “clear and conspicuous” standard could be employed to prevent companies from obscuring the information.³¹⁶ Consumer law is filled with notice requirements,³¹⁷ another could be drafted. For example, companies could be required to maintain toll-free numbers for opt-out calls.

However, there are downsides to such notices. First, they tend to suffer from some of the same deficiencies as the cable company’s Privacy Notice. Mandatory notices often contain dry, legalistic, and uninteresting prose, and offer no assurance that consumers will actually read them. Moreover, the history of mandatory notices is a checkered one: though some notices seem to have aided consumers,³¹⁸ commentators are not optimistic about their utility.³¹⁹ As indicated by the Fair Credit Reporting Act disclosures, few consumers recall seeing notices even when the notices are required to be clear and conspicuous. This suggests that when businesses do not want consumers to see a notice, consumers will not.³²⁰

The Truth-in-Lending Act offers a further cautionary tale. When first enacted in 1968,³²¹ the Act required lenders to provide consumers with a complex set of disclosures. Ambiguities in the statute and its implementing regulations

316. See Kang, *supra* note 84, at 1272.

317. See, e.g., FTC Truth-in-Lending Rescission Regulation, 12 C.F.R. § 226.15(b) (1999); FTC Holder-in-Due-Course Regulation, 16 C.F.R. § 433.2 (1999).

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

319. See generally 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); Whitford, *supra* note 253.

320. See *supra* notes 267–70 and accompanying text.

321. See Pub. L. No. 90-321, 82 Stat. 146 (1968) (codified as amended at 15 U.S.C. §§ 1601–1693 (1994)).

led to more than 1500 interpretations by 1980, as well as numerous lawsuits, often over technical questions.³²² Although the statute undoubtedly improved the manner in which information was provided to consumers, it also required that the information be presented in a format many found confusing.³²³ In 1980, Congress enacted the Truth-in-Lending Simplification and Reform Act³²⁴ primarily to fix problems with the original statute. While disclosures about information policies are likely to be less complex than disclosures about credit, the history of the Truth-in-Lending Act suggests that disclosure requirements are not always the perfect solution. In addition, the ability of the federal government to draft truly useful notices remains in doubt.

A second problem with a regulated opt-out system is that some enforcement apparatus would be necessary to ensure that businesses were living up to their obligations under the regulation.³²⁵ 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.³²⁶ Any enforcement apparatus might be both costly and difficult to administer.

Third, opt-out systems do not provide businesses with the incentive to help consumers act in accordance with their preferences. Consequently, additional regulation might be required to ensure that businesses establish opt-out mechanisms that are easy for consumers to use. Such regulation should require businesses to provide consumers with enough information to understand the mechanics of opting out and to make an informed decision.

322. See Michael M. Greenfield, *Consumer Law* 229 (1995); Pridgen, *supra* note 117, § 4.01 at 4-2.

323. See, e.g., Pridgen, *supra* note 117, § 4.01 at 4-1 to 4-2 (“[T]he disclosures were overly burdensome to creditors and too cumbersome to be of much use to the average consumer.”).

324. See Pub. L. No. 96-221, 94 Stat. 168 (1980). See generally Ralph J. Rohner, *Truth in Lending “Simplified”: Simplified?*, 56 N.Y.U. L. Rev. 999 (1981).

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

326. See *supra* notes 223–315 and accompanying text.

C. A Mandated Opt-In System

A second option requiring government intervention would be to establish an opt-in system. Such a system would reverse the current default rule.³²⁷ Obviously, those 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.³²⁸

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

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

327. "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. Interdisc. L.J.* 29, 29 (1993) ("Default rule analysts call a law a default rule if a contract could preempt it."). For an argument that opt-in rules do not run afoul of the First Amendment, see Kang, *supra* note 84, at 1277–82. See generally Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 *Cornell L. Rev.* 1756 (1995); Jonathan P. 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).

328. 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 FTC, *Privacy Online*, *supra* note 39, at 9. 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. 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.

merchants' efforts in providing a message they want the consumer to receive.³²⁹

Evidence on how companies behave in an opt-in environment suggests that such a system may be more efficient for consumers than the current system. After the FCC ruled that phone companies seeking to use phone-calling patterns for marketing purposes must first obtain the consumer's permission,³³⁰ 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 was brief, printed in different colors, and written in plain English. It also promised, in words which were underlined, that "we'll never share this information with any outside company." A postage-paid envelope and a printed form were 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 a five-dollar check, two free movie tickets, or a ten-dollar certificate from 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.

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

[T]here 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 increases 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.

330. The FCC did so in interpreting the Telecommunications Act of 1996. See 63 Fed. Reg. 20,326 (1998); see also Evan Hendricks, *FCC Backs 'Opt-In' for Phone Companies' Secondary Use of Customer Data*, *Privacy Times*, Feb. 20, 1998, at 4. The FCC's interpretation has been challenged in court. See *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (vacating FCC's order).

An opt-in system thus increases the likelihood that consumers will choose according to 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 $V_P > P + (\text{lesser of } C_{OO} \text{ and } V_{LP})$. In the opt-in scenario, the consumer who wishes to preserve his or her privacy would no longer have to take into account the transaction costs of doing so. Accordingly, under an opt-in system, the consumer should buy if the value of the product to the consumer exceeds its purchase price, or simply:

(3) consumer should buy if $V_P > P$.

The impact of opt-in systems on consumers who wish to have their personal information used should not be significant. Because 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—consumers should also purchase a product if the value to them exceeds the purchase price. Consumers who wish to opt in will have to indicate that affirmatively, instead of automatically allowing businesses to use the information. This affirmative action, however, should not require much effort. Because businesses will want consumers to opt in, they can be expected to minimize the cost of opting in. Once again, 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, thus benefiting consumers who want to receive some, but not all, solicitations. When companies have a reason to obscure opt-out provisions, as is currently the case, they have no incentive to offer mechanisms that will allow consumers to express their preferences. Returning to my personal situation, companies that do not ask me what I would like to receive will fail to learn that I want 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.³³¹

2. *Theory of Default Rules*

In regulating privacy default rules, the government should consider the theory and purpose behind default rules. In recent years, a number of scholars have written about default rules.³³² This attention was triggered in large measure by an important article by Ian Ayres and Robert Gertner.³³³ Ayres and Gertner acknowledge that transaction costs should play a role in setting defaults, but they go on to argue that in setting defaults, lawmakers 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 that give a party “an incentive to contract around the default rule.”³³⁴

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.³³⁵ “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.”³³⁶ Otherwise, Ayres and Gertner argue, 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

331. See Cavoukian & Tapscott, *supra* note 235, at 181–82.

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

333. See Ayres & Gertner, *supra* note 327.

334. *Id.* at 91.

335. See *id.* at 97.

336. *Id.* at 99.

relevant data might enable the more-knowledgeable party to end up with a larger slice of the pie.³³⁷ “When relatively informed parties strategically withhold information, courts, to promote information revelation, should choose a default that the informed party does not want.”³³⁸

Ayres and Gertner’s theory of penalty defaults is highly relevant to 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. As a result, the current system produces inefficient results.³³⁹ Changing the default gives businesses an incentive to make disclosures and increases the likelihood that an efficient market will result.³⁴⁰

3. Analogies to Negative-Option Regulation

Another reason for adopting an opt-in system is that opt-out systems, as discussed above, are analogous to negative options in that agreements are conveyed by silence. Normally, silence in commercial settings does not

337. *See id.* at 99–100. Robert Scott calls default rules adopted for such reasons “information-forcing default rules.” Robert E. Scott, *A Relational Theory of Default Rules for Commercial Contracts*, 19 J. Legal Stud. 597, 609–11 (1990); *see also* Alan Schwartz, *The Default Rule Paradigm and the Limits of Contract Law*, 3 S. Cal. Interdisc. L.J. 389, 390–91 (1993):

[L]et 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.

338. Ayres & Gertner, *supra* note 327, at 103–04.

339. 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.

340. For a thoughtful application of Ayres and Gertner’s approach to privacy in cyberspace, see Kang, *supra* note 84, at 1251–59 (concluding that default rule should be opt-in by using somewhat different analysis).

operate as acceptance of an offer.³⁴¹ Similarly, if a party to a contract suggests a change in its terms, the other party's silence does not constitute acceptance.³⁴² We do not allow sellers to impose contracts on buyers through negative options, yet we allow sellers to use consumers' personal information as they please without having to give notice.

Recognizing that negative-option agreements are troublesome, Congress and administrative agencies have regulated them in some contexts. Congress has barred cable operators from charging a consumer for services which the consumer "has not affirmatively requested."³⁴³ Similarly, there is an FTC rule that regulates the area in which negative options are probably most used, book and music clubs.³⁴⁴ The FTC rule requires that the promotional material "clearly and conspicuously disclose the material terms of the plan," including the fact that the subscriber must notify the seller if the subscriber does not wish to purchase the particular selection.³⁴⁵ The seller is also obligated to provide forms to subscribers that "clearly and conspicuously" disclose that the seller will send the subscriber the selection unless the subscriber returns the form to the seller.³⁴⁶ The negative options used in book and music clubs are significantly different from those used in information practices because book and music clubs usually notify consumers in advance of the nature of the program, and consumers voluntarily join the clubs with an understanding of how the clubs work. It seems anomalous

341. See 2 Richard A. Lord, *A Treatise on the Law of Contracts* §§ 6:3, 6:49, at 17–18, 561 (14th ed. 1991); 1 Joseph M. Perillo, *Corbin on Contracts* § 3.18, at 402–07 (rev. ed. 1993). Some exceptions appear in *Restatement (Second) of Contracts* § 69 (1981).

342. Courts will, however, sometimes infer a tacit agreement to modify a contract from silence. See *Corbin on Contracts*, *supra* note 341, § 3.18 at 564.

343. 47 U.S.C. § 543(f) (1994). This 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." 47 U.S.C. § 543(f); see also 47 C.F.R. § 76.981 (1999).

344. See 16 C.F.R. § 425 (1999).

345. 16 C.F.R. § 425.1(a)(1).

346. See 16 C.F.R. § 425.1(a)(2)(ii).

to regulate these clubs but not the information practices when it is the latter which are often unknown to consumers.

4. *Internalizing Externalities*

The sale of information is troublesome in part because it creates externalities, or costs borne by others. Externalities are created when a person engages in an activity that imposes costs on others but is not required to take those costs into account when deciding whether to pursue the activity.³⁴⁷ The feelings experienced by consumers whose information is sold and used against their wishes constitute just such externalities.³⁴⁸ An opt-in system— or an opt-out system in which consumers who object to the trade in their personal information have a genuine opportunity to opt out—can shift costs and thereby “internalize” this externality. To put it another way, consumers could bar the sale of their information unless businesses paid them an amount they deemed adequate, thereby requiring businesses selling personal information to incur a cost otherwise borne by consumers.

Businesses forced to compensate consumers for the use of their personal information would probably try to shift those costs to the purchasers of the information. Presumably, such purchasers would raise their price to compensate for any payment to consumers whose personal information they used. Hence, the purchase 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 a higher price. The higher price might reduce the number of businesses which would purchase the information, but because the higher price

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

348. See Laudon, *supra* note 87 (“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.”).

reflects the true social cost of the sale of the information, it would produce a more efficient equilibrium.³⁴⁹

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, therefore, might choose not to receive solicitations that they would have liked to receive.³⁵⁰ Consumers would also lose some of the benefits of appearing in databases.³⁵¹ However, such disadvantages can be explained to consumers at the time they decide whether or not to receive solicitations. Indeed, an opt-in system gives businesses an incentive to do just that. If consumers understand what they are giving up and still resolutely decide against opting in, their choices should be respected.

Some have argued that an opt-in system would destroy the direct-marketing industry because the cost to businesses of having consumers opt in exceeds the value to businesses of consumers' opting in.³⁵² In other words, imposing the transaction costs on businesses would make the transactions uneconomic.³⁵³ Is this true? To be

349. An example may make it clearer. Suppose the benefit of adding a particular name to a database is 80¢, and that the cost to the database company of inputting the data is 20¢ (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¢ 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¢) from the loss to the individual (\$1). 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 40¢ 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.

350. See *Privacy and the NII*, *supra* note 4, at 15–16.

351. See *supra* notes 78–98 and accompanying text.

352. See Knecht, *supra* note 213, at B1.

353. Judge Posner argues that magazines should be able to sell their subscriber lists to other magazines without obtaining the consent of their subscribers for two reasons. See Posner, *supra*

sure, each name by itself is not worth very much. Estimates of the value of individual names are usually expressed in cents, not dollars. For example, a list of 1000 subscribers to Forbes Magazine goes for \$115.³⁵⁴ Metromail reportedly charges thirty cents a name for access to its medical database containing fifteen million patients, which is useful primarily to pharmaceutical marketers.³⁵⁵ The price of e-mail addresses is even cheaper.³⁵⁶

note 53, at 398 – 99. First, the transaction costs to the magazines of obtaining consent “would be high relative to the value of the list.” *Id.* at 398; *see also* D’Amato, *supra* note 103, at 501. Second, “the costs of disclosure to the individual are small . . . [B]ecause 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.” Posner, *supra* note 53, at 398 – 99; *see also* D’Amato, *supra* note 103, at 500 (“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.” Posner, *supra* note 53, at 398.

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 128–179 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.

354. *See* Headden, *supra* note 5, at 40; *see also Report to the Congress, supra* note 27, at 8 (“Lists can range in price widely, generally anywhere from \$35 to \$250 per thousand names.”); Knecht, *supra* note 213, at B1 (stating that 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 C. Squires, *Transactions Go into a Database; Businesses Compile Dossiers on Customers*, Richmond Times Dispatch, July 28, 1996, at A-12 (noting that R.L. Polk & Co., which compiles information provided by consumers when they return product registration cards, maintains database containing some 36 million people; in recent years, it has sold its data for \$74 per 1000 names). The Lotus “Marketplace: Households” project was abandoned after consumer protests, as discussed in *supra* notes 176 –78 and accompanying text. It proposed to charge \$695 for the first 5000 names and eight cents each for additional names. *See* Branscomb, *supra* note 188, at 18.

355. *See* Kevin DeMarrais, *Big Brother Is Watching Your Database*, The Record, Apr. 30, 1995, at A1. Metromail’s lists reportedly include sufferers of asthma, diabetes, ulcers, and other illnesses. *See* Headden, *supra* note 5, at 44. 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 4, at 91. Similarly, different occupations are valued

On the other hand, some marketers appear to have paid quite a bit more in generating their lists. My local telephone company, discussed above, is just one of several examples.³⁵⁷ 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.³⁵⁸ Kay-Bee Toy Stores recently offered a five-dollar rebate to customers for their names and addresses.³⁵⁹ 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 twenty-six million names—at a cost of distributing thirty million pieces of free merchandise.³⁶⁰ These programs may have provided additional benefits to the companies beyond generating a list of smokers, but the programs undoubtedly cost much more than a few coins for each name generated.³⁶¹

There are at least two reasons why marketers may be willing to pay more for certain names than the going rate.

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 id.* One telephone company charges more for newly connected customers—\$90 or more per thousand—than for existing customers, at \$50 to \$55 per thousand. *See* Evan Hendricks, *Bell Virginia's Plan to Sell Customer Names Draws Criticism*, *Privacy Times*, Aug. 2, 1995, at 4, 5.

356. *See* Consumer Fed'n of Am., *Supplemental Comments: Unsolicited Commercial E-Mail*, in *Consumer Information Privacy Workshop* (June 18, 1997) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/ftcpriv2.htm>> (reporting that one million e-mail addresses are available for \$89; 30 million e-mail addresses are available for \$149).

357. *See supra* note 330 and accompanying text.

358. *See* Evan Hendricks, *What Price Privacy? Free PC Has an Offer*, *Privacy Times*, Feb. 15, 1999, at 3–4; *see also* Matt Richtel, *Despite Privacy Concerns, Free PCs Attract Many Consumers and Schools*, *N.Y. Times*, Feb. 25, 1999, at G7 (reporting that more than a million consumers have signed up). The company currently disclaims any intention to 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.

359. *See* Munro, *supra* note 82.

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

361. *See also* Larson, *supra* note 4, at 8–9 (“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.”).

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 useful lists. 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 list owner, who can sell (or rent) the names over and over again. A dime per name adds up over multiple sales. Hence, list owners might be willing to pay much more than just pocket change per name to buy the right to use names repeatedly, particularly if such use generates enough sales to cover transaction costs and still make a profit.

In addition, a legal regime that requires consumers to consent to the use of their names might make the names more valuable. Strategies could also 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, 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 his or her name being sold?³⁶² A system by which the subscriber

362. Judge Posner did note that some magazines seek this information. *See* Posner, *supra* note 53, at 398 n.13 (“A few magazines offer the subscriber the option of having his name 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 solicitations.”) (emphasis in original).

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

could grant or withhold such permission when he or she purchases the initial subscription or renews subsequent subscriptions need not be very expensive.³⁶³

Whether consumers would opt in under the system described above is unclear. It has been estimated that only five to ten percent of consumers would opt in.³⁶⁴ On the other hand, AOL 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; instead, they asked to be put on more lists.³⁶⁵ Also, 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 when consumer information is freely available. One company operates an opt-in e-mail system that allows consumers to be added to any of 3000 different mailing lists. Three million consumers have given their e-mail addresses to that service.³⁶⁶ The service seems to work: one of its clients increased its sales by 1000% in twelve months.³⁶⁷ Other companies offer consumers incentives to opt in to Internet solicitations.³⁶⁸ Equifax established "Buyer's

would require a publisher that 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.

363. Cf. Schwartz, *supra* note 206, at 24 (arguing that when businesses collect data in membership applications "and provide an opportunity to decline outside use of these data[,] . . . 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)").

364. See Regan, *supra* note 102, at 233; see also Posch, *supra* note 301 (quoting DMA President H. Robert Wientzen as saying: "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.>").

365. See *Information Issues*, *supra* note 192, at 41 (remarks of Ellen M. Kirsh, Vice-President and General Counsel, America Online, Inc.).

366. See FTC, *Session Two: Consumer Online Privacy I*, *supra* note 123, at 109–10 (remarks of Rosalind Resnick, President, Net Creations, Inc.). The company's website can be found at <<http://www.postmasterdirect.com>>.

367. See Letter from Rosalind Resnick, President, Net Creations, Inc., to FTC (visited Oct. 18, 1998) <<http://www.ftc.gov/bcp/privacy/wkshp97/comments2/ftcoptin.html>>.

368. For example, BonusMail, at <<http://www.mypoints.com>>, provides consumers with frequent-flyer miles and other rewards for receiving e-mail, while CyberGold, at <<http://www.cybergold.com>>, pays consumers to read ads. See Teresa Riordan, *Patents*, N.Y. Times, Feb 1, 1999, at C2.

Market,” an opt-in service under which a million consumers filled out a list of solicitations they wished to, or did not wish to, receive.³⁶⁹ The company eventually charged a modest fee for participating, but subscribers also received discounts on products.³⁷⁰ In the 1980s, National Consumer Research charged consumers \$199 to have their names and purchasing habits included in a database. The information was provided to direct marketers who provided discounts to those listed in the database. About 10,000 consumers are said to have signed up.³⁷¹

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.

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 doing so. More than twelve million people are employed in selling and advertising.³⁷² Only about 1000 people work for the two largest consumer information organizations,

369. See Larson, *supra* note 4, at 101.

370. See Mark D. Uehling, *Database Marketing: Here Comes the Perfect Mailing List*, Am. Demographics, Aug. 1991, at 10 (\$15 fee); *What Price Privacy?*, *supra* note 30, at 360; see also Blackman, *supra* note 54, at 462. In 1992, Equifax spun the division—now called Buyer’s Choice Media— off as an independent company. See Waldrop, *supra* note 228, at 46 (quoting Keith Wardell of Buyer’s Choice Media).

371. See Goodwin, *supra* note 47, at 161. Consumers also received bounties for signing up new members.

372. See Maynes, *supra* note 278, at 158.

Consumers Union (publishers of Consumer Reports) and the American Association of Retired Persons.³⁷³ 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 past cost predictions made by opponents of consumer legislation with the actual costs of such legislation once 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,³⁷⁴ it received the following testimony from the National Retail Merchants Association:

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.³⁷⁵

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 fifty-nine cents, far less than the original estimate of five dollars per letter.³⁷⁶ Similarly, when Equifax asked executives in 1990 whether ECOA had significantly increased business costs, sixty-six percent of credit-grantor executives and fifty-

373. *See id.*

374. *See* 15 U.S.C. § 1691(d)(2) (1994).

375. *Equal Credit Opportunity Act Amendments and Consumer Leasing Act: Hearings on S. 483, S. 1900, S. 1927, S. 1961, and H.R. 6516 Before the Subcomm. on Consumer Affairs of the Senate Comm. on Banking, Hous., and Urban Affairs, 94th Cong. 339 (1975)* (testimony of Robert Myers, Chairman, Legislative Steering Committee, National Retail Merchants Association).

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

nine percent of executives at banks and thrifts said it had not. Only twenty-two percent of credit-grantor executives and thirty-five percent of executives at banks and thrifts said it had.³⁷⁷ Proposals to change consumer law to protect consumers frequently attract objections based on cost estimates that later prove to be wildly inflated.³⁷⁸

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 consumers opted in. However, companies could use nonsensitive information as long as they notify consumers that such use could be prevented by sending in a form or making a telephone call before certain deadlines.³⁷⁹ NTIA acknowledges that the definition of sensitive information “is not clear-cut” and gives as examples the following: health care information, political

377. See 1990 *Equifax Report*, *supra* note 45, at 92. They were dealing with all the provisions of a statute that bars lenders from considering certain criteria in making lending decisions and asking certain questions, provides for punitive damages, and has led to other changes in lending practices. See, e.g., 15 U.S.C. § 701(a)(1) (1994) (barring lenders from discriminating on the basis of race, color, religion, national origin, sex, or marital status); 15 U.S.C. § 706 (1994) (providing for punitive damages of up to \$10,000 for individuals and up to lesser of \$50,000 or one percent of creditor’s net worth for class actions); 12 C.F.R. § 202.5(c) – (d) (1999) (implementing regulation forbidding asking of certain questions). On ECOA, see generally Greenfield, *supra* note 322, at 337–94 and Pridgen, *supra* note 117, ch. 3.

378. See, e.g., Robert J. Banta, *Negotiability in Consumer Sales: The Need for Further Study*, 53 Neb. L. Rev. 195, 196–97 (1974) (“[M]any 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.”); Daniel D. Cutler, *The Continuing Struggle for Automotive Safety*, 15 Seton Hall Legis. J. 453, 463 n.65 (1991) (stating that car manufacturers estimated airbags would cost consumers \$1100 each); 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).

379. See *Privacy and the NII*, *supra* note 4, at 15; see also Gandy, *supra* note 9, at 137 (making similar proposal).

persuasion, sexual matters, personal finances, and Social Security numbers.³⁸⁰

NTIA points out several advantages to its proposed 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 nonsensitive data, they can simply do nothing; their preferences will be accommodated by the default settings.³⁸¹ Second, the proposed system would give consumers greater control over sensitive information than they currently have.

The NTIA system may be flawed in other ways, however. 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 his or her 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."³⁸² Indeed, when the Federal Reserve System invited comments on what constitutes sensitive information, it found "widely varying answers."³⁸³ Accordingly, it may be that so many consumers would not be satisfied with the NTIA defaults

380. *Privacy and the NII*, *supra* note 4, at 25.

381. *See id.* at 26.

382. Larson, *supra* note 4, at 10.

383. *Report to the Congress*, *supra* note 27, at 14. 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. . . . [I]nformation 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 someone who has an unlisted number.

Id. at 15.

that the system would not produce any savings in transaction costs.

While the NTIA system may conform to the views of enough consumers to produce savings in transactions costs, this has not been demonstrated. It may be that a default that prevents any trade in personal information absent permission from the affected consumer more closely reflects the majority of consumers' views. Absent concrete evidence either way, it is unclear which default will produce lower transaction costs as a result of consumers' shifting away from the default.

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 should 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 should be used. This approach 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.

The incentive and ability to inflate transaction costs, however, changes the calculus. Ideally, the trigger should take into account a multitude of factors, including the cost of opting in, lost opportunities caused by consumers who would prefer to receive solicitations but do not in fact opt in (for whatever reason), the cost of strategic behavior which would occur in an opt-out system, and the cost of opting out in such a system. Given the complexity of the matter, the best approach may simply be to formulate a rule to require, unless a large percentage of consumers prefer that their information be used (perhaps as high as seventy-five percent or even higher), that personal information cannot be used unless consumers affirmatively permit it.

This approach may be most effective for information uses with which consumers generally agree. For example, comparatively few consumers object to the use of their

personal information in determining whether to accept their credit applications.³⁸⁴ Therefore, using an opt-out system in this particular context makes sense because it permits most consumers to do nothing and still attain their goals. The few consumers who do not wish to have their information used for that purpose would still have the ability to opt out. Under an opt-in system, however, most consumers would incur transaction costs while only a few consumers would benefit.³⁸⁵

V. CONCLUSION

Under the present regime, in which the trade in consumer information is largely unregulated,³⁸⁶

384. See *supra* note 138 and accompanying text. This preference is consistent with economic theory. See George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. Legal Stud. 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.

385. Cf. Ayres & Miller, *supra* note 244, at 1076 (“Requiring . . . costs disclosure when the costs of communicating are higher than the value of the information to consumers would force retailers to provide a service whose value is less than its costs.”).

386. Most uses of consumer information are unregulated. A few exceptions exist, however. For example, when Congress amended the Fair Credit Reporting Act in 1996, it created an opt-out system for prescreening. See 15 U.S.C. § 1681 (Supp. IV 1998). The statute forbids consumer reporting agencies to use information about consumers who object to the prescreening process. See 15 U.S.C. § 1681b(e) (Supp. IV 1998); see also Mass. Ann. Laws ch. 93, § 51A (Law. Co-op. Supp. 1998). The federal statute also requires consumer reporting agencies to establish a notification system for consumers to opt out. See 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 prescreening must notify the consumers whom they solicit of the consumer’s

businesses have both the incentive and the ability to inflate

right to opt out. *See* 15 U.S.C. § 1681m(d)(1)(D) – (E) (Supp. IV 1998). 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 (1994). 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. *See* 47 C.F.R. § 64.1200(e) (1999); *see also supra* note 48.

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. *See* Cal. Civ. Code § 1748.12(b) (West Supp. 1998). A card issuer must either provide cardholders with a preprinted opt-out form or maintain a toll-free telephone number for that purpose. *See* Cal. Civ. Code § 1748.12(b). The statute does not apply to information furnished to credit reporting agencies by the card issuer. *See* Cal. Civ. Code § 1748.12(e)(2) (West Supp. 1998). 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 Ann. § 59.1- 442 (Michie Supp. 1999). The merchant may give that notice “by the posting of a sign or any other reasonable method.” Va. Code Ann. § 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. *See* Act Respecting the Protection of Personal Information in the Private Sector, S.Q., ch. 17, § 13 (1993) (Can.). The president of the Commission charged with enforcing the statute reported a year after its adoption: “There has been no catastrophe in Quebec. It’s business as usual. The implementation of this important piece of legislation is running smoothly.” Cavoukian & Tapscott, *supra* note 235, at 187 (remarks of Paul-Andre Comeau, President, Commission d’Access à l’Information); *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.”).

Three states have passed statutes regulating unsolicited commercial e-mail. California and Nevada require 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. *See* Cal. Bus. & Prof. Code § 17538.4 (Deering Supp. 1999); Nev. Rev. Stat. § 41.730 (1998). 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* Wash. Rev. Code ch. 149 (1998). 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 generally* Steven Miller, Comment, *Washington’s “Spam-Killing” Statute: Does It Slaughter Privacy in the Process?*, 74 Wash. L. Rev. 453 (1999).

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 otherwise be the case if unnecessary transaction costs were eliminated. While some companies that trade in personal information are attempting to self-regulate, past failures and the atomistic nature of the consumer-information industry justify pessimism regarding the likelihood of success of such efforts. Accordingly, government should intervene to bring commercial practices more in line with consumer preferences.

That intervention should logically take one of two forms. One option is for government to preserve the existing system, but add protections to insure that consumers are adequately informed about the uses of their information and that they are given a chance to opt out of those uses. The second option is for government to impose an opt-in system in which a consumer's personal information may not be used or sold unless the affected consumer affirmatively consents.

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

Accordingly, an opt-in system is preferable, chiefly because it eliminates the incentive firms have to engage in strategic behavior and thus inflate consumer transaction costs. An opt-in system would permit consumers who wish to protect their privacy to do so without incurring transaction costs. Consumers who permit the use of their personal information should also be able to realize their wish easily. Indeed, because firms profit from the use of consumer information, firms would have an incentive to make it as easy as possible for consumers to consent to the use of their personal information. While critics of opt-in systems contend that few consumers would opt in under such a regime, this argument is without merit. Millions of consumers have already chosen to receive solicitations

under the current opt-out system. The argument overlooks the ability of businesses to persuade consumers, an ability that powers our current marketing environment. An opt-in system, therefore, seems to offer the best hope of accommodating consumer preferences while minimizing transaction costs.