ANNUAL I.H.S. - EBERHARD STUDENT WRITING COMPETITION WINNER

A CONTRACTUAL APPROACH TO DATA PRIVACY

STEVEN A. BIBAS*

We live in an information society. The computerized networks of data encircling our lives bring us myriad benefits. The free flow of credit data lets a creditor trust a borrower even if they are strangers. Nationwide computer bulletins help police capture fugitive felons. Financial market information permits investors to price goods accurately, balancing supply and demand. Communication between banks allows Californians to use their automated-teller-machine (ATM) cards in Boston or Berlin.

But every silver lining has a cloud. Although the ready availability of information helps us to trust others and coordinate actions, it also lessens our privacy. George Orwell presciently expressed our fear of losing all privacy to an omniscient Big Brother.[1] Computers today track our telephone calls, credit-card spending, plane flights, educational and employment records, medical histories, and more. Someone with free access to this information could piece together a coherent picture of our actions.

Big Brother is *not* watching—yet. The prospect, however, of easy access to personal data makes many Americans squirm.[2] The status quo poorly protects data privacy. The predictable American response has been to cry "[t]here oughta be a law"[3] and propose the creation of a federal government agency.[4] Most

* B.A., 1989, Columbia College; B.A., 1991, Oxford University; J.D. Candidate, 1994, Yale Law School. The author would like to thank Ralph Brown, John Elwood, Pavan Heard, Dan Klein, Renée Lettow, Geoff Ritts, and Eugene Volokh for their advice and comments on earlier drafts of this Article.

1. GEORGE ORWELL, 1984 (Signet Classics 1983)(1949).

2. *See infra* Part I.A.

3. Todd Purdum, *He Didn't Slash Budgets*, N.Y. TIMES, Apr. 26, 1992, § 4, at 6 (referring generally, and not in the context of data privacy, to American reliance on this "venerable democratic maxim").

4. *See* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 243 (1980)(opposing such proposals and calling them a cure "more deadly than the disease").

proposed solutions focus on centralized legislation and regulation.[5]

Portraying the choice as centrally planned government action versus doing nothing creates a false dichotomy. A contractual solution could give individuals the power to choose privacy or not without requiring privacy for everybody or nobody. This Article argues that a contractual solution would be superior to approaches dictated by legislators, bureaucrats, or judges because it would be more sensitive to individual preferences.

This Article looks only at private-sector data banks such as credit bureaus; data gathering by government agencies raises different issues.[6] Furthermore, this Article focuses on proposals limiting the dissemination of accurate data.[7] Finally, rather than speculating about the possible sale of intimate secrets,[8] this Article discusses types of information that businesses commonly handle, such as addresses and credit histories.

Part I of this Article outlines concerns about privacy and finds that Americans share no consensus on the importance of the problem. Moreover, an information economy produces large countervailing benefits. Any solution should be sensitive to individual valuations of the tradeoffs involved instead of giving privacy to everybody or nobody. Part II discusses proposed solutions involving legislation, administrative regulation, state constitutional rights, and tort law. Part III criticizes these proposals because they inefficiently ignore individual preferences and valuations. Under such regimes, some people would get less privacy than they wanted and others would get more than they wanted. Part IV sketches the legal bases for a contractual ap-

5. *See infra* Part II.A.

6. Because the government often compels disclosure by threatening to impose civil or criminal sanctions, the data giver's consent is a problematic, if not illusory, notion. The private sector, furthermore, provides data givers greater bargaining power because private businesses, unlike government organizations, usually lack monopoly power.

7. Much of the literature on data privacy confuses two analytically distinct issues by discussing privacy concerns along with concerns about false information. *See, e.g.*, Kenneth L. Karst, *"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342 (1966); Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1114-19 (1969); Lauretta E. Murdock, Comment, *The Use and Abuse of Computerized Information: Striking a Balance Between Personal Privacy Interests and Organizational Information Needs*, 44 ALB. L. REV. 589, 602 (1980); Simson L. Garfinkel, *Putting More Teeth in Consumer Rights*, CHRISTIAN SCI. MONITOR, Aug. 8, 1990, at 13; *What Price Privacy?*, CONSUMER REP., May 1991, at 356, 357. These articles stem from well-grounded complaints about the difficulties consumers face when, for instance, they try to correct inaccurate credit reports.

8. *See infra* text accompanying notes 26-28.

proach, outlines its mechanics, and discusses its benefits. This Article concludes that a contractual solution would best balance the individual's desire for privacy against the rights of others to benefit from the information economy.

I. The Privacy Problem

Many people fear the loss of their privacy in a computerized "Naked Society."[9] Others, however, are less concerned about the need for privacy and may be unwilling to sacrifice the benefits generated by the information economy. Thus, there is no consensus about the importance of privacy vis-a-vis the benefits of an information economy. One extreme solution, privacy for everybody, would deprive many people of benefits they value more highly; the other extreme, privacy for nobody, would disregard the strong privacy preference of others.[10] The law should eschew these extremes in favor of the golden mean: a solution tailored to individual preferences and values.

A. *Data Banks and the Threat to Privacy*

1. The Information Industry

Private data banks have mushroomed over the past few decades, generating a spate of dire predictions.[11] American computers hold more than five billion records. On average, they trade information on every man, woman, and child five times per day.[12] For instance, consumer credit bureaus hold 400 million credit files and make possible 1.5 million credit decisions each day.[13] More than one thousand local credit bureaus, operating through three national networks, keep files on almost ninety percent of American adults.[14] Each month, bureaus receive information about debtors from creditors; bureaus also check court records and other sources.[15] Credit bureaus contain data on con-

9. Vance Packard, The Naked Society (1964).

10. *See infra* Part III.

11. *See generally* Burnham, *supra* note 4; David F. Linowes, Privacy in America: Is Your Private Life in the Public Eye? (1989); Robert E. Smith, Privacy: How to Protect What's Left of It (1979); Malcolm Warner & Michael Stone, The Data Bank Society: Organizations, Computers and Social Freedom (1970).

12. Jeffrey Rothfeder, Privacy for Sale 17 (1992).

13. Leonard Sloane, *Credit Bureaus Draw Fire for Misuse of Data*, N.Y. Times, June 22, 1991, at 48.

14. *What Price Privacy?*, *supra* note 7, at 356. The three national bureaus are Equifax, Trans Union, and TRW. *Id.*

15. *See id.* at 356-57.

sumers' credit cards, loans, payment histories, bankruptcy liens and judgments, past addresses, years of birth, and social security numbers.[16] Credit bureaus routinely sell this information in the form of mailing lists, enabling direct-mail marketers to inundate consumers with catalogues, solicitations, and special offers.[17] In 1990, Lotus announced plans to use credit-bureau files to create a personal-computer database containing the names, addresses, demographic information, and purchasing habits of 120 million consumers.[18]

Databases are proliferating in other fields as well. Banks maintain comprehensive files on their customers' financial transactions.[19] The Employers' Information Service compiles lists of employees who have filed workers' compensation claims and lawsuits.[20] Other databases keep track of eviction filings, tenants who damage apartments, and arrests for violent and drug-related crimes. [21] The MIB, which has health records on more than fifteen million Americans, releases confidential medical information to insurance companies,[22] and another database will soon alert doctors to litigation-prone patients.[23] Two large trade groups are testing a pilot program that creates a database of people's high school records for use by employers.[24] Finally, mailing-list databases rent out individuals' names up to tens of thousands of times per year.[25]

16. *See, e.g.*, TRW CREDIT DATA SERVICES, UNDERSTANDING TRW'S CREDIT REPORTING SERVICE 2, 8 (1992); *see also* Dave Barry, *Credit Rantings*, WASH. POST, Nov. 18, 1990, Magazine, at 60; Simson L. Garfinkel, *Privacy Issue Caught in Credit Network*, CHRISTIAN SCI. MONITOR, July 18, 1990, at 1; *What Price Privacy?*, *supra* note 7, at 357.

17. *See, e.g.*, Simson L. Garfinkel, *How Computers Help Target Buyers*, CHRISTIAN SCI. MONITOR, July 25, 1990, at 13; *What Price Privacy?*, *supra* note 7, at 359-60.

18. Mary J. Culnan, *An Issue of Consumer Privacy*, N.Y. TIMES, Mar. 31, 1992, § 3, at 9. Lotus has cancelled this product, perhaps because of public complaints about the product's impact on their privacy. *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 (stating that Lotus "could be forced to pull or delay the product" because of compaints).

19. *See* SMITH, *supra* note 11, at 15-28.

20. Richard Lacayo, *Nowhere to Hide*, TIME, Nov. 11, 1991, at 34.

21. Simson L. Garfinkel, *From Database to Blacklist*, CHRISTIAN SCI. MONITOR, Aug. 1, 1990, at 12.

22. *Id.* The MIB was formerly known as the Medical Information Bureau. *Id.* For an interesting look at medical privacy, see Ted Cantrell, *Privacy—The Medical Problems*, *in* PRIVACY 195 (John B. Young ed., 1978).

23. Tamar Lewin, *Philadelphia Doctors to Be Offered Data on Patients Who Have Sued*, N.Y. TIMES, Aug. 27, 1993, at A21.

24. Lacayo, *supra* note 20, at 35.

25. ROTHFEDER, *supra* note 12, at 90.

Databases, however, do not contain everything about you. Contrary to one writer's suggestion, Big Brother does not know about "every sexual fantasy you [have] had."[26] Credit bureaus, for instance, do not contain data on one's friends, relatives, religion, cultural tastes, political affiliation, or sexual orientation.[27] Thus a credit bureau knows only "a very small part of the basic facts about a consumer's existence, facts that a casual acquaintance might know."[28] Reform proposals should focus on commonly traded types of business information instead of being distracted by sensationalist Orwellian claims about issues like sexual privacy.

2. The State of the Law

The law imposes almost no restrictions on the sale of accurate information. Databases may freely disclose information about employment, criminal records, and tenants. No federal law protects medical privacy, although Congress has considered such legislation.[29] No federal law safeguards the privacy of insurance files.[30] The only federal law on the privacy of bank information forbids disclosure to the government but does not restrict sale to private parties.[31] Laws place a few limits on the disclosure of videocassette rentals,[32] educational records,[33] and cable television data,[34] but there is no evidence that these were ever major

26. Barry, *supra* note 16, at 60 (all capitalized in original).

27. *See* TRW CREDIT DATA SERVICES, *supra* note 16, at 2; Daniel B. Klein & Jason Richner, *In Defense of the Credit Bureau*, 12 CATO J. 393, 397 (1992).

28. Klein & Richner, *supra* note 27, at 397.

29. ROTHFEDER, *supra* note 12, at 177.

30. *Id.* at 27.

31. *See* Right to Financial Privacy Act, 12 U.S.C. §§ 3401-34 (1988) (limiting conditions under which government institutions may obtain bank records; giving customers a right to authorize disclosure in writing and to revoke authorization at any time; and prohibiting banks from requiring such authorization as condition of doing business).

32. *See* Video Privacy Protection Act, 18 U.S.C. § 2710 (1988) (forbidding disclosure of videocassette rental records except under court order, subpoena, warrant, or with express contemporaneous written consent of consumer; requiring destruction of personally identifiable information after one year; but permitting sale of names and addresses and past rentals "if the disclosure is for the exclusive use of marketing goods and services directly to the consumer"). This last loophole practically swallows the protection of the section.

33. *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1988) (pertaining to federally-funded schools) (guaranteeing parents access to educational records and forbidding release of such records to others without written consent, subject to specified exceptions). *But cf.* Fay v. South Colonie Cent. Sch. Dist., 802 F.2d 21 (2d Cir. 1986) (holding that the Act creates no private cause of action).

34. *See* Cable Communications Policy Act, 47 U.S.C. § 551 (1988) (prohibiting cable operators from gathering or disclosing personally identifiable information without subscriber's prior consent unless (a) necessary for "a legitimate business activity," (b) required by court order, or (c) viewing habits are blocked out; also requiring cable

sectors of the data trade.[35] Although the Fair Credit Reporting Act ostensibly limits disclosures by credit bureaus,[36] some courts have restricted its application to inaccurate information.[37] The statute, furthermore, permits a bureau to release a consumer credit report to anyone deemed to have "a legitimate business need" for the information.[38] This exception has swallowed the statute.[39] Thus credit bureaus routinely sell mailing lists, lists of good debtors, and the like, without the slightest hindrance from the law.[40]

State laws also fail to protect data privacy. Although many states have made tortious the public disclosure of private facts,[41] these torts only cover highly offensive, private matters of no legit-

---

operators to destroy personally identifiable information once retention is no longer necessary).

35. The author has been unable to find a single case involving the commercial sale of videocassette rentals, educational records, or cable television data.

36. *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (1988) (limiting permissible reasons for releasing credit reports, forbidding reporting of obsolete information, and requiring user of consumer credit reports to notify consumer when credit-report information causes user to deny consumer credit).

37. *See* Todd v. Associated Credit Bureau Servs., Inc., 451 F. Supp. 447, 449 (E.D. Pa. 1977) (holding that court need not reach issue of reasonableness if, as threshold matter, credit report was accurate), *aff'd*, 578 F.2d 1376 (3d Cir.), *cert. denied*, 439 U.S. 1068 (1978); Roseman v. Retail Credit Co., 428 F. Supp. 643, 646 (E.D. Pa. 1977) (holding that an accurate report was not actionable because FCRA sought "to protect consumers from having inaccurate information circulated concerning them"); Austin v. Bankamerica Serv. Corp., 419 F. Supp. 730, 732-33 (N.D. Ga. 1974) (holding that accurate report does not violate FCRA); *see also* Pendleton v. Trans Union Sys. Corp., 76 F.R.D. 192, 195 (E.D. Pa. 1977) (denying class-action certification because of need to show that each class member suffered inaccuracy); Virginia G. Maurer, *Common Law Defamation and the Fair Credit Reporting Act*, 72 GEO. L.J. 95, 124 (1984) (stating that "in general, courts are unwilling to permit actions under section 1681o when the information in the report is true").

38. *See* 15 U.S.C. § 1681b (1988) (limiting consumer credit report disclosure to situations involving court orders, written instructions by the consumer, creditors, employers, insurers, government benefit programs, and others having "a legitimate business need").

39. ROTHFEDER, *supra* note 12, at 55, 57 (stating that the bill "has been butchered; it was drawn and quartered and its vitals were left on the committee's chopping block" by the insertion of "[t]his remarkably broad exception" at the urging of industry lobbyists (quoting Professor Arthur Miller of Harvard Law School)); *see also* Bonnie G. Camden, Comment, *Fair Credit Reporting Act: What You Don't Know May Hurt You*, 57 U. CIN. L. REV. 267, 267 (1988) ("The [Fair Credit Reporting Act], as interpreted today, frequently allows dissemination of credit reports to people without a legitimate need for the reports."). Businesses, furthermore, have evaded the Act's strictures by obtaining reports for purposes not listed in the statute. According to some courts, such reports are not "consumer reports" and thus fall outside the statute. *See, e.g.*, Houghton v. New Jersey Mfrs. Ins. Co., 795 F.2d 1144, 1148-49 (3d Cir. 1986) (holding that report obtained by insurance company about claimant's financial status was not consumer report because no consumer relationship existed between plaintiff and defendant); Henry v. Forbes, 433 F. Supp. 5, 6, 8 (D. Minn. 1976) (finding that report obtained by attorney for use in lobbying was not consumer report because it was not prepared for one of the specific statutory purposes).

40. ROTHFEDER, *supra* note 12, at 26, 98 (noting that, for decades, industry has been selling lists of consumers without hindrance by the Fair Credit Reporting Act).

41. *See generally* RESTATEMENT (SECOND) OF TORTS § 652D (1963 & App. 1977-1989).

imate public concern.[42] Typically, data dissemination does not involve publicity as courts have defined the term,[43] and it rarely involves highly offensive matters. As a result, "courts have usually rejected [privacy-tort] claims based on information privacy."[44] Thus neither state nor federal law provides much data privacy protection.

3. Privacy Concerns

Many people care about data privacy. In a 1990 poll, seventy-nine percent of those polled were concerned about their personal privacy.[45] Almost half of those surveyed thought "technology had gotten out of control."[46] Even a decade ago, one third of Americans feared that we were on the verge of an Orwellian society lacking all privacy.[47] Reacting to this crisis, Congress has considered several data-privacy bills in recent years.[48]

Several themes recur in the complaints of privacy advocates. First, data subjects are unaware of the use of their data.[49] Second,

---

42. *Id.*

43. Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1413 (1987) (citing Santiesteban v. Goodyear Tire & Rubber Co., 306 F.2d 9, 11 (5th Cir. 1962)).

44. *Id.*

45. *What Price Privacy?*, *supra* note 7, at 356 (summarizing results of 1990 Harris poll commissioned by Equifax, Inc.).

46. *Id.*

47. LOUIS HARRIS & ASSOCIATES, INC. & ALAN F. WESTIN, THE DIMENSIONS OF PRIVACY 5 (1981).

48. *See, e.g.*, Consumer Reporting Reform Act, S. 783, 103d Cong., 1st Sess. (1993); Consumer Reporting Reform Act, H.R. 1015, 103d Cong., 1st Sess. (1993); Credit Reporting Agencies Accuracy of Consumer Information Act, H.R. 619, 103d Cong., 1st Sess. (1993); Fair Credit Reporting Amendments, H.R. 630, 103d Cong., 1st Sess. (1993); Individual Privacy Protection Act, H.R. 135, 103d Cong., 1st Sess. (1993).

Congress has considered other bills. The Consumer Credit Reporting Act would have tighted restrictions on the use and sale of credit reports. *Time for Credit Horror Stories to End*, L.A. TIMES, Aug. 9, 1992, at M4 (noting that the bill will be considered in 1993). Representatives Richard Lehman, Charles Schumer, and Matthew Rinaldo have introduced bills to tighten access to credit reports. The bills would both limit marketers' access to reports and require deletion of old information. Garfinkel, *Putting More Teeth in Consumer Rights*, *supra* note 7, at 13; *see also* Michael W. Miller, *Credit-Reporting Industry Will Launch Campaign to Forestall New Regulations*, WALL ST. J., June 5, 1991, at B1 (stating that Congress at that time was considering five bills that would have tightened access to credit reports). Representative Bob Wise has introduced a proposal to create a federal data-protection board. Lacayo, *supra* note 20, at 35. At least three Congressional committees have held hearings on personal-data gathering. *See* Michael W. Miller, *Hot Lists: Data Mills Delve Deep to Find Information About Us Consumers*, WALL ST. J., Mar. 14, 1991, at A1. Finally, Representative Schumer has sponsored a bill to curtail tenant-screening networks. Pam Belluck, *Tenants Cry Foul as Screening Companies Help Landlords Spot 'Problem' Applicants*, WALL ST. J., Dec. 27, 1985, at 13.

49. Culnan, *supra* note 18, at 9; Garfinkel, *How Computers Help Target Buyers*, *supra* note 17, at 13.

data gatherers routinely use information gathered ostensibly for one purpose, such as getting credit, for other purposes unanticipated by the data subject, such as employment and mailing lists.[50] Finally, data subjects lack control over what happens after they release information.[51]

B. *The Untold Side of the Story*

1. There Is No Consensus on the Importance of Privacy

"[O]ur society is at least ambivalent about the [importance of] personal privacy," because individuals' rights to privacy conflict with others' rights to know the truth.[52] As one writer stated, "[i]t's hard to find a national consensus on confidentiality in a nation of tell-all memoirs, inquiring pollsters and talk shows . . . ."[53] Half of those surveyed did not fear the improper use of information by business.[54] Privacy, moreover, is a very subjective and mutable concept. "What is private to one individual may not be private to his neighbor; what is considered private today may not be considered private tomorrow."[55] Thus, Americans share no consensus about the value of privacy.[56]

2. The Benefits of an Information Economy

The uninhibited flow of financial information makes possible the liberal provision of credit.[57] It enables creditors to trust consumers about whom they have no first-hand knowledge.[58] Accu-

50. *See, e.g.*, Garfinkel, *How Computers Help Target Buyers*, *supra* note 17, at 13; Lacayo, *supra* note 20, at 36 (discussing use of warranty-registration cards to generate stereo- and record-company mailing lists); Jacob Sullum, *Secrets for Sale: Do Strangers with Computers Know Too Much About You?*, REASON, Apr. 1992, at 28, 32 (noting that privacy advocates argue "the first rule of informational privacy [is]: Information disclosed for one purpose should not be used for another purpose without the subject's consent").

51. *See* Culnan, *supra* note 18, at 9; Mendel-Black & Richards, *supra* note 18, at H1.

52. Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 326 (1983).

53. Lacayo, *supra* note 20, at 34.

54. LOUIS HARRIS & ASSOCIATES, INC. & WESTIN, *supra* note 47, at 5 (finding that 50% of those surveyed in 1978 did not worry about business misuse of personal information).

55. ERIK LARSON, THE NAKED CONSUMER 10 (1992).

56. This lack of consensus holds true even if one assumes that one-third of the unconcerned 50% (*see supra* note 54) are unconcerned solely because they are ignorant about how information is sold. Under such an assumption, 33% of the consumers would not care about the diminution of data privacy.

57. Jeremiah Smith, *Conditional Privilege for Mercantile Agencies*—Macintosh v. Dun pt. 1, 14 COLUM. L. REV. 187, 199 (1914); Stephen Chapman, *Credit Report: Friend or Foe?*, WASH. TIMES, June 10, 1991, at F2; *see also* Fair Credit Reporting Act, 15 U.S.C. § 1681(a)(1) (1988); H. Hart, *Privacy in the Financial Field*, *in* PRIVACY, *supra* note 22, at 259, 279.

58. Klein & Richner, *supra* note 27, at 396-97.

rate credit-history information allows creditors to charge lower interest rates to reliable debtors, thus encouraging all debtors to keep their promises. By turning consumers into repeat players, information networks overcome the incentives to cheat creditors in a prisoner's dilemma.[59] Individuals benefit as well as businesses. Even one staunch critic of data dissemination admits that credit bureaus make it possible for the middle class to obtain both credit and lower prices.[60] Thus, people with sound credit ratings have reason to favor the dissemination of their credit histories.

The same logic applies to networks of landlords and employers: The dissemination of truthful information rewards good tenants and employees and punishes defaulters and shirkers. Tenants who default on rent and damage apartments create costs that landlords pass on to other tenants. Tenants who turn their apartments into brothels or shops for illegal drugs worsen the quality of life for other tenants. Information networks allow landlords to screen out bad tenants, saving good tenants money and keeping out criminal activity and nuisances.[61]

Even the much-maligned junk-mail industry serves a purpose. Many consumers enjoy receiving mailings and shopping at home.[62] Mail-order shopping is convenient for those with small

59. *See* Daniel B. Klein, *Promise Keeping in the Great Society: A Model of Credit Information Sharing*, 4 ECON. & POL. 117 (1992). *See generally* ROBERT AXELROD, THE EVOLUTION OF COOPERATION (1984) (demonstrating the importance of knowledge of past behavior and reciprocity in overcoming prisoner's dilemmas).

The prisoner's dilemma is the name given to certain types of coordination problems in which each participant has an incentive to act selfishly even though cooperation would maximize their joint welfare. For a common example, suppose that the police have arrested two thieves. The police take the prisoners into separate interrogation rooms and seek to make each one confess and testify against the other prisoner. If both prisoners remain silent, each will serve two years in jail. If one prisoner confesses while the other remains silent, the confessing prisoner will go free while the other prisoner will serve six years. If both prisoners confess, each prisoner will serve five years in jail. Under these circumstances, each prisoner has an incentive to confess and thus serve either zero or five years instead of two or six years. The best joint outcome would be for both thieves to remain silent and serve two years each; however, because of the coordination problem, the thieves probably will not both remain silent. For a numerical version of this scenario, see *id.* at 8-10.

60. ROTHFEDER, *supra* note 12, at 43.

61. *See* Belluck, *supra* note 48, at 11. *But cf.* Garfinkel, *From Database to Blacklist*, *supra* note 21 (reciting anecdotal complaints of tenants and attorneys concerning tenant databases).

62. Daniel Klein & Jason Richner, *In Defense of that Pesky Junk Mail*, CHI. TRIB., Apr. 20, 1992, § 1, at 19; *see also* LINOWES, *supra* note 11, at 153. Some consumers actually pay money to have their names put on certain mailing lists. *What Price Privacy?*, *supra* note 7, at 360. One study finds that 88% of people accept direct mail when they have the option of discontinuing it. Klein & Richner, *supra*, at 19.

children, physical disabilities, or insufficient time to go to stores.[63] Strengthening the mail-order industry creates manufacturing jobs and reduces pollution and traffic congestion, because consumers no longer have to drive to malls.[64] More precise information enables marketers to target only those consumers most likely to want to receive particular mailings, thereby reducing mailing costs and conserving paper.[65]

We must balance the value of the information industry against its costs in order to decide under what circumstances privacy is worthwhile. Because tradeoffs are involved, the law should avoid conferring too much privacy or too little. Any solution should reflect individuals' varying valuations of privacy and the countervailing benefits.[66]

II. Proposed Solutions

Legislators and pundits have proposed data-privacy solutions involving legislation, regulation, state constitutional rights, and tort law. These approaches would require government officials to decide for everyone what tradeoffs are worth making for privacy. The proposals' centralized, one-size-fits-all solutions contrast with this Article's individuated solution.

A. *Legislative and Regulatory Solutions*

Some commentators have called for Congress to enact stringent statutory measures.[67] Each of the past four Congresses has considered legislation to establish a federal Data Protection Board.[68] The Consumer Credit Reporting Act, considered in

63. Klein & Richner, *supra* note 62, at 19.

64. *See id.*

65. *Id.*

66. *See infra* Part III (discussing how centralized solutions fall into the all-or-nothing trap).

67. *See, e.g.*, Computer Professionals for Social Responsibility & U.S. Privacy Council, 1991 Report, *quoted in* Sullum, *supra* note 50, at 30 (supporting a stringent legislative solution); Larson, *supra* note 55, at 237-39 (arguing for a flexible Omnibus Privacy Act and a constitutional privacy amendment); Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers, 185, 213, 220-38 (1971) (arguing that instead of leaving responsibility to individuals and letting "placebo" of consent operate, government should set up statutes or regulations); Alan F. Westin, Privacy and Freedom 386-88 (1970) (advocating detailed legislative planning and administrative rules); Miller, *supra* note 7, at 1170, 1229-44 (proposing tightening of statutory protection); Camden, *supra* note 39, at 292 (same); Murdock, *supra* note 7, at 610 (advocating federal legislation and administrative agency).

68. *See* H.R. 685, 102d Cong., 1st Sess. (1991); H.R. 3669, 101st Cong., 1st Sess. (1989); H.R. 638, 100th Cong., 1st Sess. (1987); H.R. 1721, 99th Cong., 1st Sess. (1985).

1993, would have tightened restrictions on the use and sale of credit reports.[69] Congress, moreover, has recently held a flurry of hearings on possible restrictions on the sale of consumer data.[70]

Others argue that Congress should pass enabling legislation to allow administrative regulations and an independent agency or commissioner to regulate data privacy.[71] This administrative approach parallels that of many European countries, which have passed data-privacy legislation setting up centralized data protection boards.[72] One purported virtue of the administrative approach is its flexibility and responsiveness to technological changes and new threats.[73] Spiros Simitis argues that laws should

---

69. *Time for Credit Horror Stories to End*, *supra* note 48, at A24.

70. At least three congressional committees have held hearings on the subject. *See* Miller, *Hot Lists: Data Mills Delve Deep to Find Information About Us Consumers*, *supra* note 48, at A1.

71. *See* Miller, *supra* note 7, at 1236; Kenneth J. Langan, Note, *Computer Matching Programs: A Threat to Privacy?*, 15 COLUM. J.L. & SOC. PROBS. 143, 177-78 (1979); Murdock, *supra* note 7, at 610.

72. In 1984, Britain adopted the Data Protection Act. *See* Data Protection Act, 1984, ch. 35 (Eng.). It requires data gatherers to register with a Data Protection Registrar. *Id.* §§ 4-5. Data subjects enjoy rights of access to data, compensation for unauthorized disclosure or access or inaccurate data, and correction or erasure of inaccurate or misleading data. *Id.* §§ 21-24. Data users must follow eight data protection principles: 1) One must get and process information fairly and lawfully. 2) One may only hold it for specified and lawful purposes. 3) Data must be adequate, relevant, and not excessive in relation to that purpose. 4) One may not use data for purposes other than those for which one gathered it. 5) Data must be accurate. 6) One must not keep data longer than necessary. 7) One must inform data subjects of the existence of data on them and give them rights of access and correction. 8) Finally, data bureaus must take appropriate security measures. *Id.* sched. I, pt. 1; *see also* J.A.L. STERLING, THE DATA PROTECTION ACT 1984: A GUIDE TO THE NEW LEGISLATION ¶¶ 1250, 1260 (1985); Ian J. Lloyd, *The Data Protection Act—Little Brother Fights Back?*, 48 MOD. L. REV. 190, 192-93 (1985).

Other countries have similar centralized solutions. The Irish Data Protection Act of 1988 employs the same eight principles as the British Act. *See* ROBERT CLARK, DATA PROTECTION LAW IN IRELAND 18, 45-57 (1990). *Compare* Irish Data Protection Act, No. 25 (1988) (Ir.) *and* Data Protection Act, 1984, ch. 35 (Eng.) *with* Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg 1981) (showing that all three acts share nearly identical wording of eight principles). The Irish Act also sets up a Data Protection Commissioner to enforce compliance. The Irish system pays little attention to individual wishes: "The entry on the register rather than the wishes of the data subject determine [sic] how use and disclosure is to be policed by the Commissioner." CLARK, *supra*, at 18. The European Union has considered a proposed directive on data privacy. It would have required member states to set up a centralized supervisory authority to which data gatherers would have had to report. Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1990 O.J. (C 277) 3, 7, 11. *Cf.* Proposal for a Council Directive Concerning the Protection of Personal Data and Privacy in the Context of Public Digital Telecommunications Networks, in Particular the Integrated Services Digital Network (ISDN) and Public Digital Mobile Networks, 1990 O.J. (C 277) 12. Germany, Norway, and Austria have set up data protection commissioners or central executive agencies. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 745 (1987).

73. *See* Miller, *supra* note 7, at 1236; Murdock, *supra* note 7, at 618.

set up independent commissioners capable of continually updating regulations.[74] Countries, he says, need a "mandatory framework" insensitive to individual wishes, because data subjects "cannot determine the proper data processing conditions."[75] This mindset, paradoxically, ignores individuality in the name of protecting individuals.

B. *Constitutional Protection of Data Privacy*

Several authors have suggested that the constitutional right of due process protects an individual's liberty interest in privacy or property interest in controlling personal information.[76] Although the U.S. Supreme Court has never squarely addressed this argument, dicta in *Whalen v. Roe*[77] suggest that such an argument might succeed.

In *Whalen*, the Court upheld New York's maintenance and use of a computer database listing users of certain prescription drugs against liberty and privacy challenges under the Fourteenth Amendment.[78] The Court, however, "[r]ecogniz[ed] that in some circumstances [the] duty [to avoid unwarranted disclosure of data] arguably has its roots in the Constitution."[79] Because this case involved state action, the current Court is unlikely to extend any such due process right into a property interest enforceable against private parties.[80] A constitutional solution, however, re-

74. Simitis, *supra* note 72, at 741-43, 745.

75. *Id.* at 736-37.

76. *See* Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. Rev 133, 135 (1991) (advocating both liberty and property protection and the use of an intermediate scrutiny analysis). Two other commentators have suggested similar proposals but have restricted their foci to privacy rights against the government. *See* Robert S. Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 Hofstra L. Rev. 893, 898 (1984) (advocating extension of constitutional right to privacy to "withholding personal information" from the government); Heyward C. Hosch III, Note, *The Interest in Limiting the Disclosure of Personal Information: A Constitutional Analysis*, 36 Vand. L. Rev. 141, 142-43, 179 (1983) (arguing "for the establishment of a fourteenth amendment liberty interest in limited disclosure" protected by rational relation review). One other author has argued for the constitutional recognition of a property right in information, though he has not applied that theory to individual privacy. *See* Michael A. Dryja, *Information as Property: Philosophy, Economics, and the Constitution*, 25-41 (Oct. 1992) (unpublished manuscript, on file with the Harv. J.L. & Pub. Pol'y).

77. 429 U.S. 602 (1977).

78. *Id.* at 603-04 & n.32.

79. *Id.* at 605. Concurring, Justice Brennan put this point even more strongly: "[T]he Constitution puts limits . . . on the means [the state] may use to gather" information. *Id.* at 607 (Brennan, J., concurring).

80. The Fourteenth Amendment's protection of life, liberty, and property only extends to deprivation by state action; it does not forbid purely private conduct. *See* Jackson v. Metropolitan Edison Co., 419 U.S. 345 (1974) (limiting state action to traditional public functions and duties and refusing to extend doctrine to all businesses affected with public

mains feasible because state courts could interpret their state constitutions to protect privacy even in the absence of state action.[81]

C. *The Tort of Commercial Dissemination of Private Facts*

One commentator has rejected statutory solutions because "the inflexible nature of an across-the-board statutory remedy might render the remedy inadequate to deal with the fluid nature of the information economy."[82] Applauding the flexibility, innovative capacity, and insulation of courts, he has proposed making tortious the "unacceptable . . . commercial dissemination of private facts."[83] He justifies the creation of this tort on the basis of the perceived "violat[ion of] our society's shared expectations of privacy."[84] Under this approach, courts would "evaluate the quality of the information exchanged" and decide what "necessary and beneficial" dissemination merits protection.[85] Courts can best balance individual privacy interests against the public benefits of dissemination, he argues.[86] This author provides few concrete details about how judges and juries should handle this task.

III. Problems with Centralized Approaches

The statutory, constitutional, and tort solutions do not respect individual perceptions and valuations of privacy. They adopt Simitis' view that "[w]hether or not the details of the intended retrieval are explained to them . . . [data subjects] cannot determine the proper data processing conditions."[87] The tort solution, for example, requires judges to balance the utility of dissemination against the value of privacy to a reasonable person. It thus

interest). *See generally* Geoffrey R. Stone et al., Constitutional Law 1593-1661 (2d ed. 1991).

81. For instance, the California Constitution protects privacy. *See* Cal. Const. art. I, § 1 (listing right of privacy as inalienable right of all people). The California Supreme Court has suggested that this protection applies against corporations as well as against the government. *See* White v. Davis, 533 P.2d 222, 234 (Cal. 1975) (en banc) (stating in dictum that the legislative history of the privacy amendment shows that it embraces "overbroad collection and retention [and improper use] of unnecessary personal information by government and business interests"); 7 Bernard E. Witkin, Summary of California Law § 454 (9th ed. 1988) (same).

82. Graham, *supra* note 43, at 1424.

83. *Id.* at 1426, 1428, 1430.

84. *Id.* at 1430.

85. *Id.* at 1428, 1430.

86. *Id.* at 1423 & n.149.

87. Simitis, *supra* note 72, at 736; *see supra* text accompanying note 75.

implicitly relies on a societal judgment about the unacceptability of particular disclosures.[88] Any such uniform standard based on the preferences of a non-existent reasonable person would imperfectly assess and allocate the social costs of withholding information. People's individual valuations of privacy vary greatly from those of a reasonable person.[89] A tort solution, therefore, would give those who place a high value on privacy less of it than they desire and those indifferent to privacy more of it than they want.[90]

Price theory buttresses this argument. As Nobel Laureate economist Friedrich von Hayek notes, there is no objective scale of values for commodities.[91] Therefore, central planning cannot "compare or assess the relative importance of needs of different persons."[92] Because "demand is built up of innumerable incommensurable scales of valuation," centralized solutions cannot take into account and satisfy "individuals' subjective valuations" and tradeoffs.[93] Central plans, therefore, would allocate resources inefficiently:[94] They would keep some information private although it would be worth more to merchants, and they would permit dissemination of other data the privacy of which people value highly. Each such case, whether it involves the release of too little information or too much, would produce an inefficient outcome.

In contrast, the price mechanism takes into account individual values, needs, and tradeoffs, allocating resources to their most-valued uses.[95] Pricing, unlike central planning, respects consumer preferences.[96] It adjusts resource-allocation decisions to maximize value and swiftly takes changed circumstances into ac-

88. *See supra* text accompanying notes 84-86.

89. *See supra* Part I.B.1.

90. Of course, this is true of all torts. The law-and-economics explanation for why the law imposes tort liability is that "transaction costs with potential victims . . . are prohibitive." RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 164 (4th ed. 1992). That rationale does not apply here because the data subject and data gatherer communicate and can bargain freely (except perhaps in a monopoly situation).

91. Friedrich A. von Hayek, *Socialist Calculation I: The Nature and History of the Problem, in* INDIVIDUALISM AND ECONOMIC ORDER 119, 137 (1949).

92. *Id.*

93. Georg Halm, *Further Considerations on the Possibility of Adequate Calculation in a Socialist Community* (H.E. Batson trans.), *in* COLLECTIVIST ECONOMIC PLANNING 131, 183 (Friedrich A. von Hayek ed., 1935).

94. *Id.* at 145.

95. *Id.* at 141, 145.

96. Friedrich A. von Hayek, *The Present State of the Debate, in* COLLECTIVIST ECONOMIC PLANNING, *supra* note 93, at 201, 215.

count.[97] It is a prerequisite for rational economic decisions: "Without a pricing mechanism, there is no economic calculation."[98] A contractual approach, by pricing information, would thus more efficiently allocate data than would a centrally planned solution.

The importance of varied individual preferences becomes clearer if one considers a hypothetical: A mail-order retailer holds data on ten consumers' buying habits. The ten consumers attach widely differing values to the privacy of their buying habits. C_1 values her privacy at \$1, C_2 values his privacy at \$2, and so on up to C_{10}, who values her privacy at \$10. A typical merchant, M, values each set of data at \$6.50. One blanket rule for this scenario would offer no privacy because M's valuation is higher than those of the majority of the consumers. Such a one-size-fits-all rule is insensitive to individual wishes. C_7, C_8, C_9, and C_{10} respectively value their privacy \$0.50, \$1.50, \$2.50, and \$3.50 more than M values their information, yet they cannot protect their privacy. If instead the blanket rule protected everyone's privacy, C_1 through C_6 would receive privacy that is worth less to them than the information is worth to M. From an efficiency standpoint, information should be put to its most-valued use. Therefore, the latter rule would inefficiently deny M access to some of the data.

Ideally, a solution should fit its problem. In the case of regulation of the information industry, perceptions and valuations of the privacy problem vary too greatly for a conventional, centralized solution to fit well. We must therefore turn to the branch of the common law most sensitive to individual preferences: contracts.

IV. A Contractual Solution

A. *The Common Law*

Contracting parties, in theory, may freely draw up contracts specifying conditions of confidentiality.[99] Classical contract law alone, however, will not solve the privacy problem. Individuals release information in standard form contracts yet lack the

97. Friedrich A. von Hayek, *The Use of Knowledge in Society*, *in* Individualism and Economic Order, *supra* note 91, at 77, 87, 103.

98. Ludwig von Mises, *Die Wirtschaftsrechnung im sozialistischen Gemeinwesen*, 47 Archiv für Sozialwissenschaften (1920), *translated and reprinted as Economic Calculation in the Socialist Commonwealth* (S. Adler trans.), *in* Collectivist Economic Planning, *supra* note 93, at 87, 111.

99. *See* Gordon Hughes, Data Protection in Australia 224-29 (1991).

power to renegotiate these contracts. Unequal bargaining power[100] and start-up transaction costs prevent individual consumers from insisting on contractual rights to privacy.[101] No one business will absorb the costs of redrafting standard forms, implementing privacy procedures, and educating consumers.[102]

B. *How Contractual Data Privacy Would Work*

A federal statute would require users of standard form contracts to include an opt-in or opt-out clause.[103] The clause would govern release of information that the data subject disclosed to the data gatherer on that form or in later transactions pursuant to that form.[104] The penalty for failure to include such an option

100. MILLER, *supra* note 67, at 214.

101. In most transactions, the value of privacy to consumers, while significant, is probably dwarfed by the start-up transaction costs involved and by other considerations. For example, an individual desiring a Visa card will accept a bank's standard no-privacy terms when the cost of renegotiating the standard terms exceeds the difference between the value of privacy to the individual and the value of information to the bank. This is true even if his privacy is worth more to him than the information is worth to the bank.

Additionally, consumers face enforcement problems. See *infra* note 108 for this Article's free-market enforcement scheme. A privacy right is worth little to consumers if there is no enforcement mechanism to back it up. It might not be worth the trouble for businesses to start up privacy schemes because consumers would have no assurance that businesses were delivering the promised privacy. There is a chicken-and-egg problem here: Information sleuths (enforcers) will not come into existence until there is a big enough market to assure steady business and allow for economies of scale. Consumers, however, will not demand contractual privacy rights until there is an enforcement industry to make those rights meaningful. This Article's proposal would solve this quandary by creating a flood of privacy rights at once, thus encouraging information sleuths to commit time and capital to building up enforcement businesses.

102. There may be isolated circumstances where transaction costs are so low and privacy is worth so much to consumers that a business will offer options of its own accord. In most industries, however, the start-up cost of establishing options and unilaterally informing consumers about their options would exceed the goodwill gained by the business. Although spreading the consumer-education costs over all businesses would reduce the cost, the transaction costs of coordinating education expenditures would be prohibitively high.

103. The choice of an opt-in or opt-out clause would be tied to the selection of a default rule. *See infra* note 106. If the default rule provided privacy, the form would have an opt-out clause; otherwise it would have an opt-in clause.

104. For example, if a consumer requested privacy on a credit-card application, the credit-card company would have to keep private all information disclosed on that form and disclosed in the course of subsequent credit-card purchases.

Special problems arise in the credit context because credit bureaus do not contract directly with debtors. Presumably credit bureaus could be made parties to the contract on an agency theory. The credit-card companies would contract as agents of the credit bureaus. Under the law of agency for partially disclosed or undisclosed principals, both the credit-card companies and credit bureaus would be bound by the terms of the contracts. *See* RESTATEMENT (SECOND) OF AGENCY §§ 144, 186, 321-22 (1958). Alternatively, the credit-card companies could fully disclose their principals by naming the credit bureaus to which they planned to disclose data. They could then contract to bind their principals to secrecy (on an agency theory) and additionally contract to bind themselves (under an ordinary bilateral contract). *See id.* §§ 144, 320.

would be imposition of an implied contractual duty not to spread the information outside the corporation or other entity.[105] The default rule (governing those who did not sign the clause)[106] would match the prevailing expectations and practices in that type of business.[107] Public ignorance might necessitate a public-service advertisement campaign to inform people of their privacy rights. Market incentives would encourage private agents to police privacy violations.[108]

---

105. Thus, businesses that had no desire to disseminate information could save the cost of including the clause.

106. A default rule is a rule that fills gaps in contracts. It would specify, for a particular type of form, either that failure to sign the clause will result in privacy protection or that it will not. The orthodox view in contract law is that the law should set default terms at what most parties would have chosen had they explicitly addressed the issue. *See, e.g.*, POSNER, *supra* note 90, at 93; Charles J. Goetz & Robert E. Scott, *The Mitigation Principle: Toward a General Theory of Contractual Obligation*, 69 VA. L. REV. 967, 971 (1983); *see also* Lewis v. Benedict Coal Corp., 361 U.S. 459, 468-69 (1960) (applying this approach to setoffs of pension contributions). Ian Ayres and Robert Gertner, however, have noted that sometimes it is more efficient for the law to choose default rules that do not mimic parties' hypothetical desires. Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 91 (1989). Two of their considerations apply to the information industry. First, consumers desiring privacy are probably more likely to contract around a no-privacy default than consumers not desiring privacy are to contract around a privacy default. This factor weighs in favor of setting the default rule at no privacy. *See id.* at 93. Second, many consumers are unlikely to know of a no-privacy default. This factor supports setting the default rule at privacy, so that businesses have to inform the uninformed consumers to get them to opt out of privacy. *See id.* at 98. These two considerations point in opposite directions and, absent empirical evidence to the contrary, would seem to cancel each other out. The logical solution, therefore, would minimize the disruption of business by setting the default equal to whatever the currently prevailing norms are in an industry: for example, bank accounts would enjoy privacy (and so would have opt-out clauses) but magazine subscriptions would not (and so would have opt-in clauses).

107. Presumably Congress would ascertain these business expectations by making use of an investigatory subcommittee or independent agency. But these default rules should not be constantly revised; to respect contracting parties' expectations and reliance, the law should be stable and secure.

108. Instead of relying on an inefficient government body to police violations, this contractual scheme would generate policing by a band of information sleuths. (Data subjects could sue as well, but proving violations would be difficult unless the data subject had released a particular datum to only one business.) Entrepreneurs would submit decoy entries to various data banks via pseudonymous credit card applications, magazine subscriptions, insurance applications, and the like. On the forms, the sleuths would request privacy for all information. If the decoys began receiving mail from outside the data-gathering corporation, the sleuths would have proof of a violation and could sue for damages. These damages should be set at a statutory sum of liquidated damages plus attorney's fees because it would be impossible to prove the quantum of actual damages. The attorney's fees provision would be analogous to the law of derivative shareholder suits against corporations. *See, e.g.*, REVISED MODEL BUSINESS CORP. ACT § 7.46 (1984). The fee award would encourage attorneys to police violations, turning them into private attorneys general.

One could supplement this sleuthing scheme with rewards for whistle-blowing employees who revealed breaches of contractual privacy.

Users of standard forms would then have to offer inducements for the right to sell information, leading the market to price privacy efficiently. Market pricing would allocate information to its most-valued uses. Although a statute would provide the impetus, this approach would not be centrally planned; rather, the valuations and tradeoffs would rest on individuals' choices instead of blanket statutory determinations. It is impossible to tell *a priori* whether this solution would increase or decrease the flow of data, but that inquiry is irrelevant. What matters, as Part III argues, is that market pricing based on individual preferences would cause information to flow to its most-valued uses.

The market's treatment of silence will depend upon the type of data and the circumstances of the silence. With some types of data, such as mailing lists, data buyers will be unable to tell that an individual has opted for privacy (as opposed to not being listed in a database in the first place). The market, therefore, will not draw adverse inferences from a person's choosing privacy. In many other situations, many people will opt for privacy because they value it highly. When many people do so, the market will only read that choice as indicating that people value their privacy highly. The market under these circumstances will not impose significant costs on privacy.

The interesting case occurs when most people value their privacy very little: Only those with something to hide and extreme privacy lovers (call them hermits) will choose privacy. In such situations, the market will read opting for privacy as a sign of concealment of damaging facts. It will then spread the costs of the presumed damaging facts (for example, bad credit history) over the privacy choosers (for example, by charging higher interest rates). Those concealing damaging facts deserve to pay this premium, because as Posner notes, "others have a legitimate interest in unmasking the deception" and charging concealers accurate rates.[109] But what of the hermit? As noted above, centralized solutions rest on shared social expectations of what should be private[110] and therefore would deny the hermit any privacy beyond what the majority wants. Because the majority will

109. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 395, 399-400 (1978) (stating that individuals have interest in discovering truth of those they deal with instead of taking deceptive representations at face value and that inquiry is a way of unmasking exploitation, misrepresentation, and misapprehension).

110. *See supra* Part III.A.

care little about privacy in this situation,[111] a centrally planned solution would offer the hermit no privacy. The hermit, therefore, would prefer the contractual solution because it would allow her to choose to buy her privacy if she wishes.[112]

C. *Advantages of a Contractual Approach*

In the hands of bureaucrats or judges, flexibility produces uncertainty for private parties. In the hands of the contracting parties, however, flexibility allows people to control their lives and efficiently tailor the law to meet their needs. Flexibility is the market's forte; the pricing mechanism is extremely sensitive to variations in valuation and quickly adjusts to them.

This flexibility would produce contractual changes even though consumers would have only two choices. Imagine a hypothetical: Congress has set the default rule for mail-order vendors at no privacy. The Book-of-the-Month Club has ten customers, C_1 through C_{10}, most of whom loathe telephone solicitations but do not care as much about junk mail. Table I displays a possible set of merchant valuations of telephone numbers and addresses and consumer valuations of privacy for the two types of information.

111. The scenario in this paragraph postulated (in the first sentence) that the majority cared little about privacy in this situation. The reasoning in the text holds true for any situation in which fewer than half of all people care about privacy. The contractual solution, unlike a centralized one, respects both majority and minority preferences.

112. In contrast, a blanket solution would impose privacy on everyone for the sake of the hermit. Thus all consumers, regardless of whether or not they valued privacy highly, would have to pay a premium that reflected the costs imposed by the deceivers. This specter also raises the danger of faction: A well-organized minority could sate its privacy preferences by imposing privacy on everyone. This minority would spread privacy costs to the privacy-apathetic majority even though the latter would be unwilling to pay that much for privacy. It is fairer to impose any social costs on those most desiring privacy instead of inflicting them on everyone without regard to individual preferences.

By making individuals bear the costs of privacy, moreover, the contractual solution would make each person reflect on how much he valued privacy. This argument does not rest on the overriding importance of the social benefits of data flow. It rests on requiring individuals to weigh serious tradeoffs instead of imposing their own preferences upon others with different valuations. The market would impose no undue penalty; its pricing would reflect the value of information, and individuals would be free to choose for themselves whether privacy is worth the costs.

TABLE I: HYPOTHETICAL VALUATIONS OF INFORMATION
Book-of-the-Month Club and Its Customers

Value to:	Merchant	C_1 and C_2	C_3, C_4, C_5, C_6, C_7, and C_8	C_9 and C_{10}
Type of Information:				
Telephone Number	$2	$2	$6	$11
Address	$7	$2	$4	$8
Total Value	$9	$4	$10	$19

If the Book Club offers the choices:

1) no privacy plus five dollars, or
2) complete privacy,

eight of the ten consumers will contract for privacy because the privacy is worth more than five dollars to them. The Book Club will pay each of the remaining two consumers five dollars for their addresses and telephone numbers, sell these data for nine dollars per person, and make an eight dollar profit. The Book Club, however, can make more money if it unilaterally promises not to disclose *anyone's* telephone number. If it offers the options:

1) telephone-number privacy plus five dollars, or
2) complete privacy,

then only two privacy lovers will contract for complete privacy. The other eight consumers will choose not to opt out. The Book Club, therefore, will pay each of these eight consumers five dollars, sell their addresses for seven dollars, and make a sixteen dollar profit. The Book Club will prefer the latter scenario and will promise not to release telephone numbers. The threat of opting out by members on the margin will lead the Book Club to tailor its default disclosure terms to average consumer valuations.[113] Similarly, the desire to keep consumers on the margin from opting out will lead information holders to offer inducements to all consumers. If preferences and values change, moreover, the price mechanism will lead parties to reallocate information

113. Not only would this system better reflect average preferences, but it would also provide a way out for those on the privacy-preferring end of the spectrum.

The Book Club could, in theory, achieve the same result by offering consumers an option for telephone-number privacy as well as a total-privacy option. But the additional costs of drafting and handling new forms would probably make this option impractical.

rights. No centralized solution can match the flexibility and dynamism of this contractual approach.

Conclusion

We value the "right 'to be let alone.'"[114] We also value the right to reap the benefits of an information economy. One-size-fits-all proposals ignore the individual valuations and tradeoffs involved. They give privacy lovers too little privacy and those indifferent to privacy too much privacy.[115]

By enabling people to contract for their optimal mix of privacy and financial benefits, government could leave it to the market to price privacy efficiently. The market would allocate information to its most-valued uses instead of forcing privacy into a Procrustean bed. The answer to *Consumer Reports*' rhetorical question, "What Price Privacy?,"[116] should be: whatever price the market will bear.

114. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890) (quoting Thomas Cooley, Law of Torts 29 (Chicago, Callaghan & Co., 2d ed. 1888)).

115. *See supra* Part III.

116. *What Price Privacy?*, *supra* note 7.