2004

Nonprofit Fundraising and Consumer Protection: A Donor's Right to Privacy

Ely R. Levy

Norman I. Silber
Maurice A. Deane School of Law at Hofstra University

NONPROFIT FUNDRAISING AND CONSUMER PROTECTION: A DONOR'S RIGHT TO PRIVACY

Ely R. Levy* and Norman I. Silber+

* J.D., Hofstra University School of Law, 2003; BA, New York University, 2000.
+ Professor of Law, Hofstra University School of Law.

I. INTRODUCTION: PERSONAL INFORMATION AND PRIVACY

This Article explores the privacy concerns that arise when nonprofit fundraisers trade, sell, rent or otherwise exploit personal information about charitable donors that they obtain in the course of obtaining donations. Drawing from the experience of consumers in the sales context,[1] it considers whether donors who make gifts should be equated with consumers who make purchases, and therefore should fall within the reach of traditional and statutory consumer privacy protections. Part I briefly explores the jurisprudence of privacy and developing concern about the divulgence of personal information by private corporations, including nonprofit corporations. Part II addresses the contemporary market for personal information. The practice of compiling, selling, and renting charitable donor lists is addressed specifically. Part III considers consumer concerns, economic benefits, as well as the commercial interest in this trade. Part IV addresses the theoretical and case law bases for comparing donors to consumers.

Part V discusses government responses to the problems associated with this trade, including key consumer protection statutes and their shortcomings. Part VI describes the administrative avenues of redress that might be open to charitable donors, but are not. This Part demonstrates how, with respect to the sale of charitable donor lists, there is little if anything the Federal Trade Commission (FTC) or state attorneys general are doing at present to protect donor privacy. Additionally, this Part explains problems consumers and donors have faced in the judicial arena, particularly in light of the recent New York Appellate Division decision, *Smith v. Chase Manhattan Bank.*[2]

The Authors conclude that at least in the context of informational privacy, the interests of donors essentially mirror those of consumers. Consumers and donors alike have a strong interest in maintaining the privacy of their personal information. Any distinction based on the difference between a gift and a sale fails to take into account the purpose of all privacy laws, namely, to control the dissemination of personal information without the consent of the persons about

---

[1] *See infra* notes 92-119 and accompanying text.

[2] 741 N.Y.S.2d 100 (N.Y. App. Div. 2002).

whom the information is collected, or, as Justice Brandeis insisted more than a century ago, the assurance of the right to be let alone.[3] Moreover, considering important public policy objectives, which include the encouragement of donations and of gratuitous undertakings, as well as maintaining public trust in nonprofit organizations, this Article argues that protecting the private information of donors should be treated as tantamount to protecting the personal information of consumers.

Having presented the case for protecting the privacy rights of donors, and having explained the failure to do so until the present time, the Authors suggest three ways to proceed. This Article makes the case for the extension to donors of federal opt-out protections similar to those currently available in some commercial contexts. It proposes limitations on the collection and use of personal data about donors by nonprofit organizations, including a "do not share" registry; and it suggests a federal statutory right of action that would give individual donors a right of action against organizations, which, against the will of donors, share personal information.

A. *The Jurisprudence of Privacy*

As a law student and later as a Justice on the Supreme Court, Louis Brandeis championed a broad constitutional and common law right to privacy. The formulation he used in his pioneering 1890 article, The Right to Privacy,[4] embraced different personal concerns, such as a claim for common law protection of privacy based on tort theories and contract theories, including breach of confidence[5] actions to protect what today is referred to as personal information privacy or consumer privacy. Although Brandeis did not receive

---

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). The article was written, as the famous story goes, in response to officious news coverage of Brandeis daughter's wedding. The Authors claimed that the right of privacy with respect to ordinary behavior in everyday life existed independently of the form in which publication of such behavior took place. They provided this example:

> A man writes a dozen letters to different people. No person would be permitted to publish a list of the letters written . . . . The copyright of a series of paintings or etchings would prevent a reproduction of the paintings as pictures; but it would not prevent a publication of a list or even a description of them. Yet in the famous case of Prince Albert v. Strange, the court held that the common-law rule prohibited not merely the reproduction of the etchings which the plaintiff and Queen Victoria had made for their own pleasure, but also the "publishing . . . a description of them, whether more or less limited or summary, whether in the form of a catalogue or otherwise."

Id. at 201-02.

[4] *See id.*

[5] "[I]n some instances where protection has been afforded against wrongful publication, the jurisdiction has been asserted, not on the ground of property . . . but upon the ground of an alleged breach of an implied contract or of a trust or confidence." *Id.* at 207 (citing *Abernethy v. Hutchinson*, 3 L.J. Ch. 209 (1825) where the court granted an injunction against publication of a surgeon's lectures on the ground of breach of confidence and trust). For a discussion on the privacy torts, see generally, RESTATEMENT (SECOND) OF TORTS § 652 (1977).

immediate support for his views on this subject, the High Court over the next half-century endorsed many of them. In 1928 he enshrined his law review argument in a Supreme Court dissent. "The right to be let alone [is] the most comprehensive of rights and the right most valued by a [free people]," he wrote.[6]

By 1951, the Court had moved considerably toward the Brandeis position. Notwithstanding important First Amendment concerns, Justice Reed, in *Breard v. Alexandria*, presented the view that

> [t]here is . . . unanimity that opportunists, for private gain, cannot be permitted to arm themselves with an acceptable principle, such as . . . a privilege to engage in interstate commerce, or a free press, and proceed to use it as an iron standard to smooth their path by crushing the living rights of others to privacy and repose.[7]

Later, in *Katz v. United States,*[8] *Griswold v. Connecticut,*[9] and other cases, the Court legitimized the existence of an individual's right to a "reasonable expectation" of privacy in contexts other than those of the consumer marketplace.[10] A privacy right has been invoked in the Court's protection of

---

[6] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[7] 341 U.S. 622, 625-26 (1951) (upholding a local prohibition on door-to-door sales solicitations).

[8] 389 U.S. 347 (1967) (legitimizing the term "privacy" and holding that citizens have rights to their "reasonable" and/or "legitimate" expectations of privacy in the Fourth Amendment search and seizure context).

[9] 381 U.S. 479 (1965) (holding that there is a fundamental right to privacy that prohibits laws criminalizing birth control and further construing the privacy right as one that implicitly exists in the "penumbra of the Bill of Rights").

[10] The reasonable expectation of privacy paradigm has been discussed in many different contexts. *See, e.g.*, Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 394 (2002) (stating that the reasonable expectation of privacy framework has been applied to protect only information that expresses identity and not personal information per se); Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503 (2001) (arguing that government encryption without a search warrant cannot violate the Fourth Amendment); Patricia Mell, *Big Brother at the Door: Balancing National Security With Privacy Under the USA PATRIOT Act*, 80 DENV. U. L. REV. 375 (2002) (discussing the right to privacy as it relates to issues of national security); Robert C. Post, *Rereading Warren and Brandeis: Privacy, Property, and Appropriation*, 41 CASE W. RES. L. REV. 647 (1991) (discussing privacy in the context of tort actions); Radhika Rao, *Property, Privacy and the Human Body*, 80 B.U. L. REV. 359 (2000) (exploring the application of the constitutional right to privacy to the human body); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993) (providing social science data to suggest that expectations of privacy and autonomy reflect realistic societal attitudes); Daniel J. Solove, *Remedying Privacy Wrongs—New Models: Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227 (2003) (arguing that the problems associated with the expectation of privacy and identify theft have not been adequately conceptualized, thereby leading to misdirected enforcement efforts); Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751 (1994). Several scholars contend that the Supreme

interests in areas including bodily privacy,[11] informational privacy,[12] membership in political groups,[13] privacy in physical places,[14] and decisional privacy.[15]

The Rehnquist Court in recent years has been more protective of commercial speech rights than previous courts, and it has been none too zealous about the protection of privacy in several fields of law.[16] Nonetheless,

---

Court's emphasis on a reasonable expectation of privacy is flawed. *See, e.g.*, Tracey Maclin, *The Decline of the Right of Locomotion: The Fourth Amendment on the Streets*, 75 CORNELL L. REV. 1258, 1328-30 (1990); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583 (1989).

[11] *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973) (holding that the fundamental right to privacy implicit in the Fourteenth Amendment invalidates blanket prohibitions on abortion).

[12] *See, e.g.*, Reno v. Condon, 528 U.S. 141 (2000) (upholding the privacy of personally identifiable driver information and the federal Drivers Privacy Protection Act, 18 U.S.C. § 2721 (2000); Whalen v. Roe, 429 U.S. 589 (1977) (asserting a Fourteenth Amendment privacy interest requiring confidentiality to protect prescription drug use information collected by states).

[13] *See, e.g.*, Stanley v. Georgia, 394 U.S. 557 (1969) (recognizing the right to privacy in the context of personal use of pornography in one's own home); NAACP v. Alabama, 357 U.S. 449 (1958) (upholding a privacy interest in membership lists relating to the right of organization members to pursue their interests privately).

[14] *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709 (1987) (upholding the privacy of government employee's office, desk, and files); Payton v. New York, 445 U.S. 573, 602-03 (1980) (finding arrest warrant mandatory for home arrests because of a heightened privacy expectation); Miller v. United States, 357 U.S. 301 (1958) (upholding privacy rights in one's home). *But cf.* Florida v. Riley, 488 U.S. 445, 450 (1989) (holding that flying over one's backyard is not protected by the Fourth Amendment); California v. Greenwood, 486 U.S. 35, 40-41 (1988) (holding that rummaging through one's garbage is not protected by the Fourth Amendment); California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (same); Chambers v. Maroney, 399 U.S. 42, 47-48 (1970) (holding that motor vehicles have a reduced expectation of privacy). For an interesting discussion on employee privacy in the workplace, see Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT L. REV. 271 (1996).

[15] *See, e.g.*, Paul v. Davis, 424 U.S. 693, 713 (1976) (recognizing decisional privacy interests in familial contexts—child rearing, marriage and procreation); Loving v. Virginia, 388 U.S. 1 (1967) (recognizing privacy and equality interests in interracial marriages); Griswold v. Connecticut, 381 U.S. 479 (1965); Prince v. Massachusetts, 321 U.S. 158, 166 (1944) (holding that family relationships are within the realm of privacy that the state cannot regulate); Skinner v. Oklahoma, 316 U.S. 535, 541 (1942) (holding that the power to sterilize is a violation of a person's ability to procreate, which is a fundamental liberty); Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (holding that the right to teach children different languages is a protected right under the Fourteenth Amendment). *But cf.* Washington v. Glucksberg, 521 U.S. 702 (1997) (declining to recognize a right to physician assisted suicide that would invalidate state laws criminalizing that activity); Cruzan v. Missouri Dept. of Pub. Health, 497 U.S. 261 (1990) (holding the states may require families to demonstrate by clear and convincing evidence that a patient is in a hopeless persistent vegetative state prior to terminating life support).

[16] "In this cluster of 'privacy related' cases, the [Rehnquist] Court has described the specific right in question in liberty terms rather than in privacy terms. Under the Rehnquist Court, privacy nomenclature rarely occurs, and individual rights are treated directly as part of the liberty that is protected by the Due Process Clauses of the Fifth and Fourteenth Amendments." G. Sidney Buchanan, *A Very Rational Court*, 30 HOUS. L. REV. 1509, 1571-

the Court has upheld the validity of several consumer privacy statutes designed to limit marketing practices and collection tactics used by commercial enterprises—statutes that have limited the right of commercial parties to gather and share information about individuals and that have been passed by state and federal legislatures.[17] The enactment and judicial defense of privacy provisions contained in the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, the Telemarketing Privacy Act, the Bank Privacy Act, and the Health Insurance Portability and Accountability Act, and also the expansion of common law tort remedies in the area of unwanted publicity and privacy, manifest unusually assertive legislative and judicial action on behalf of civil liberty—especially unusual given recent trends, post-September 11, to sanction invasions of privacy by government in the interest of security.[18]

Appreciation for the strength of the consumer right to privacy in the private sphere should be tempered by recognition of its significant limitations. State and federal statutes address the informational privacy of consumers with respect to certain invasive behaviors, but the protections they offer are idiosyncratic. For example, information about the video cassette rental

---

72 (1993). While the right to privacy in the Rehnquist era has been "thus far and no further," the Court recently upheld the privacy rights of homosexuals in *Lawrence v. Texas*, 123 S. Ct. 2472 (2003). Writing for the majority, Justice Kennedy stated: "When homosexual conduct is made criminal by the law of the State, that declaration in and of itself is an invitation to subject homosexual persons to discrimination both in the public and private spheres. The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime." *Id.* at 2482.

[17] *See* Trans Union Corp. v. FTC, 245 F.3d 809 (D.C. Cir. 2001) *cert. denied*, 536 U.S. 915 (upholding the constitutionality of the privacy sections of the Fair Credit Reporting Act, 15 U.S.C. § 1681 (2000), by dismissing a First Amendment challenge to mailing list regulations); Individual Reference Servs. Group, Inc. v. FTC, 145 F. Supp. 2d 6 (D.D.C. 2001) (upholding the privacy regulations under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2000) and stating that the regulations did not violate plaintiffs' right to free speech under the First Amendment, as the regulations serve a substantial state interest, directly and materially advanced that interest, and were no more extensive than necessary to do so); *see also*, Kenro Inc. v. Fax Daily, Inc., 962 F. Supp. 1162 (S.D. Ind. 1997) (rejecting a First Amendment constitutional challenge to the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2000) and upholding the statute's ban on the transmission of unsolicited fax advertisements). Privacy advocates have several future hurdles to overcome.

Recently the American Telemarketing Association launched challenges to the Federal Trade Commission's (FTC) latest privacy rights effort—the "do not call" database. A complaint was filed in federal court in Colorado challenging the "do not call" scheme on First Amendment grounds. *See* Press Release, Am. Telemarketing Ass'n, ATA Launches Legal Challenge Against New Rules (Jan. 3, 2003), *at* http://www.donotcall.com/lawsuit.asp. Ultimately, the Tenth Circuit, in *Mainstream Marketing Services Inc. v. FTC*, 358 F.3d 1228 (10th Cir. 2004), overturned a lower court's decision that invalidated the do-not-call database on First Amendment grounds. These cases will be discussed in greater detail in Part VII *infra*.

[18] *See* Ann Davis, *Data Collection Is Up Sharply Following 9/11*, WALL ST. J., May 22, 2003, at B1 (discussing government national security efforts and initiatives aimed at tracking movements and personal backgrounds of everyday Americans).

practices of consumers is protected by federal statute,[19] but the ability of satellite television networks to monitor and analyze viewing data is not. The sharing of information about creditworthiness that is collected by "credit reporting agencies" is regulated by state and federal statutes; but gathering and distributing of financial information by other entities from bankruptcy filings or court proceedings generally is not covered.[20] There is no broad all-encompassing statute that addresses general consumer rights to privacy.[21]

B. *The Nonprofit Privacy Gap*

Absent from most available legal privacy protections, however, are rules that protect the privacy of donors who make charitable gifts to donees, particularly to nonprofit organizations.[22] The major privacy protection rules speak mainly to the regulation of the use by *sellers* or *vendors* of information obtained from *purchasers* or *consumers*; they do not regulate the use by *donees* of personal information they have about nonprofit *members, clients,* and *donors*.[23] Furthermore, the privacy constraints on commercial solicitation generally do not apply with respect to activities by nonprofit solicitors and fundraisers.[24] As distinguished from the commercial context, infringement of

---

[19] The Video Privacy Protection Act, 18 U.S.C. § 2710 (2000), prohibits disclosure of consumer video rental records.

[20] *See* Peter C. Alexander & Kelly Jo Slone, *Thinking About the Private Matters in Public Documents: Bankruptcy Privacy in an Electronic Age*, 75 AM. BANKR. L.J. 437, 439 (2001) (arguing for Congress to address the privacy of debtors whose financial information and bankruptcy status is susceptible to public intrusion by anyone with access to the bankruptcy court PACER web system); Mark D. Bloom et al., *Reorganizing in a Fish Bowl: Public Access vs. Protecting Confidential Information*, 73 AM. BANKR. L.J. 775 (1999).

A separate and distinct privacy issue in the bankruptcy arena is the legal treatment of a corporate debtor's privacy policies in bankruptcy. How privacy policies are treated in bankruptcy proceedings currently hinges on whether such policies are viewed as creating contract rights or property rights. When courts perceive the debtor's privacy policies as a contract obligation, thereby subjecting them to discharge in bankruptcy, consumer expectations of privacy are usually compromised. For a comprehensive article on this recent issue, see generally, Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801 (2003).

[21] *See infra* notes 120-28 and accompanying text.

[22] For purposes of this Article, donors should be considered de facto consumers, who, spontaneously or subsequent to solicitations, decide to make gifts to nonprofit organizations, corporate or noncorporate, tax-deductible or otherwise. And *donees* are recipients of donated funds who do not offer consideration in return for assets they receive from donors but are often qualified to provide donors with deductions from their income taxes in proportion to the size of their gifts. *See generally* BORIS I. BITTKER, FEDERAL TAXATION OF INCOME, ESTATES, AND GIFTS 5 (1981).

[23] For a more comprehensive discussion on the consumer/donor distinction see *infra* notes 78-91 and accompanying text. Unless otherwise indicated, this Article will include "clients" and "members" under the heading of "donors."

[24] The FTC has exempted solicitations inducing charitable contributions via outbound telephone calls from the "do-not-call" registry provision of the Telemarketing Sales Rule

the privacy of donors is largely unprotected.

Add to the unremediated infringement of the privacy interests of donors the increasingly privileged treatment of nonprofit and for-profit telemarketing rights; add again the increasing ease with which gathered information about donors can be turned to business advantage; and compound with the pervasiveness of nonprofit fundraising activities. The combined effect is the generation of an explosive growth in the nonprofit exploitation of personal information about donors. Rights, as the legal theorist Joseph Singer has written, do not actually extend further than "the scope of the remedies the law will grant to right-holders."[25] By this standard (except, as will be noted below, for those rights that benefit donors incidentally because they apply to entire types of business activity), today's donors to nonprofit organizations make their gifts without specific privacy rights.

II. THE CONTROVERSIAL LIST TRADE

Trading in personal information about consumers and donors has become pattern and practice.[26] "Data-mining" has become more valuable, in all

---

(TSR). *See* Fed. Trade Comm'n, Loopholes in the National Do-Not-Call Registry, *at* http://www.donotcall.com/loopholes.asp (last visited Apr. 20, 2004). Only the less restrictive entity-specific "do-not-call" provision requiring telemarketers to maintain their own "do-not-call" list and to honor consumers' requests to be placed on that list and receive no further calls will apply to charitable solicitation telemarketing. *See* FTC Release, FTC Announces Final Amendments to Telemarketing Sales Rule, Including National "Do Not Call" Registry (Dec. 18, 2002), *at* http://www.ftc.gov/opa/2002/12/donotcall.htm.

[25] Joseph William Singer, *Starting Property*, 46 ST. LOUIS U. L.J. 565, 575 (2002).

[26] The Minnesota Attorney General's website contains several illustrations of how prevalent and sophisticated the trade in personal information has become in recent years:

> One company maintains a database that operates twenty-four hours a day, gathering and processing information on 95% of American households. For a price, it will sort information based on income, lifestyle (outdoor, mechanic, intelligence, etc.), or even a profile of "ethnics who may speak their native language but do not think in that manner."
>
> Another company offers lists of people with particular medical conditions. In 1999, it offered for sale nearly 50 lists of individuals suffering from different medical ailments. It sells the names and addresses of 427,000 people who are clinically depressed, 1.4 million women who have yeast infections, and 1 million individuals who have diabetes. It also sells lists of people with Alzheimer's Disease, birth defects, Parkinson's Disease, and "physical handicaps."
>
> A New York company offers the names of high school students according to GPA, religion, ethnicity, and SAT scores.
>
> A hospital sells the names of its patients who may be eligible for Social Security insurance to a lawyer.
>
> No information appears to be too personal for companies to collect or too insignificant to sell. In 1999, electronic research companies were selling unlisted phone numbers for $49, social security numbers for $49, and bank balances for $45. A company will obtain another person's driving record for $35, trace a cell phone call for $84, or create a list of stocks, bonds, and securities for $209. This personal data is merged into a consumer tracking and information system that becomes larger every day it is sold to whomever may be interested in buying. Each piece of information gathered, stored, and sorted by these large databases represents an erosion of your right to privacy.

Office of the Minnesota Attorney General, Guarding Your Privacy, *at* http://www.ag.state.

respects, than ever: it is widely used by organizations to improve their own operating results, and may be traded or sold by them for gain. An almost endless variety of information is of interest: items such as the identity of consumers and donors; their earnings; their net wealth; their general giving practices; their history of giving to particular organizations; their friends and associates; their estate plans; their publicly available addresses; their private addresses; their internet, facsimile, telephonic, and wireless contact information; their ages; their educational levels; their marital status; their occupations; their height, weight, and other physical characteristics; their religion; their ethnicity;[27] their gender; their credit standing; their volunteer activity in philanthropic causes; their hobbies; their political affiliations; the stores they shop in; the personal purchases they make; their newspaper and magazine subscriptions; the location of their second homes; and much other information. The acquisition and processing of this information has been facilitated by the newer technologies, and serves the financial and mission-oriented interests of nonprofits. There is also a benefit flowing to consumers and donors through the intra-organizational sharing of information with third parties. The retention and use of this information, however, also intrudes upon privacy rights and heightens the likelihood that individuals will be barraged with junk mail and spam, embarrassed, annoyed, defrauded, or even will have their identities stolen.[28]

A. *Profiling Simplified*

The sophistication with which personal information is compiled and analyzed has increased rapidly in the last decade.[29] The rise of information

---

mn.us/consumer/Privacy/GuardingYPrivacy/GYP_1.htm (last visited Apr. 20, 2004).

[27] Regarding the collection of ethnic data, opponents of affirmative action programs in California have sought to stop the dissemination of ethnic information by way of popular initiative. In October 2002, Californians voted on a "Racial Privacy Initiative" that if passed, would have barred state and local government entities from maintaining databases containing ethnic information of citizens. This initiative that would have barred the collection of ethnic information on forms involving school enrollment, government contracting, and job applications, did not pass. *See* Robert Tomsho, *Some Seek Ban on Collection of Ethnic Data*, WALL ST. J., June 30, 2003, at B1.

[28] The seriousness and increasing incidence of the identity theft crime has prompted the President and several members of Congress to pursue a broad range of consumer-friendly measures aimed at reducing the incidence of identity theft by curtailing the personal information trade, particularly with respect to financial information. *See* Rebecca Christie, *Identity-Theft Safeguards Proposed*, WALL ST. J., July 1, 2003, at D3.

[29] *See, e.g.*, Sandra Byrd Petersen, *Your Life As an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163 (1995); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) (describing the use of the Internet in facilitating the personal information trade); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1396, 1398 (2001) (discussing the role of databases in the information trade and describing the traders as being part of a "clandestine underworld"); Jeff Sovern, *Protecting Privacy with*

technology, networking, and the Internet significantly expanded available personal information. The proliferation of computers and sophisticated data processing software has also encouraged gathering and dissemination through sophisticated collection techniques, corporate outsourcing of data processing, and the establishment of information service providers and clearinghouses.[30]

Crucial to the marketing success of both for-profit and nonprofit organizations is the cultivation and acquisition of lists. Corporations go as far as to create a profile of individuals by compiling lists of people with particular characteristics and purchasing histories.[31] Obtaining, refining, and exploiting lists has become an economic consideration relevant to nearly every company's bottom line—a significant expense for enterprises that market to consumers, both for-profit and nonprofit, and a significant part of the income stream for many of them as well.[32]

Companies and associations of all sizes seek out list brokers, rent lists, and use those lists to solicit new members, donors, subscribers, clients, or purchasers of nonprofit services. Larger organizations—nonprofit and for-profit—use their own databases to compile lists and then to "cross-market" by soliciting persons who already have some association with the organization. Lists usually qualify as depreciable assets for tax and accounting purposes, and the expenses from the purchase of lists are frequently classified on corporate and nonprofit ledgers against marketing and fundraising accounts.

Lists are readily compiled because almost all consumer and business transactions leave behind some sort of electronic record. Sources of information include credit card transactions, mortgage records, magazine subscription information, birth records, warranty cards, purchase plans, and driver registration records.[33] Marketing agencies and other similar entities collect layers of information and form multiple profiles of individuals and their "electronic persona[s]."[34] Similarly, almost all nonprofit donations,

---

Deceptive Trade Practices Legislation, 69 FORDHAM L. REV. 1305, 1307 (2001) (discussing the different ways companies have acquired and disseminated personal information).

[30] *See* Allen R. Grogan & Ron Ben-Yehuda, *Outsourcing Data Processing Operations*, 8 COMPUTER L. 1 (1991); *see also* John Markoff, *Business Technology: For Shakespeare, Just Log On*, N.Y. TIMES, July 3, 1991, at D1 (describing data exchange networks). The fear that databases would sophisticate the personal information trade was contemplated as early as the 1970s. *See* ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY 3-5 (1972).

[31] *See* Sovern, *supra* note 29, at 1309.

[32] *See id.* at 1307. Interestingly enough, many European countries have attempted to curtail these practices. Austria, France, Germany, Ireland, and the United Kingdom have broad statutes that provide a general set of privacy rights applicable to the private sector. *See* A.C. Evans, *European Data Protection Laws*, 29 AM. J. COMP. L. 578 (1991); *see also Data Protection Roundup*, PRIVACY L. & BUS., July 1991, at 2-7.

[33] *See* William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 960 (1996).

[34] *See* Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 606-07 (1994) (proposing a statute mandating that all consumer transactions

membership subscriptions, opinion communications, and requests for services leave behind some sort of electronic record. Sources of information include pledges, membership applications, contribution forms, feedback forms, fundraising replies, newsletter and magazine subscription forms and applications, the registration of Internet browsing choices, and membership surveys. The nonprofit "electronic persona" may be no less sophisticated and complex than the commercial one.

The nature of profiles that are available to be purchased is often amusing and sometimes alarming. For instance, one can purchase a list of people who have purchased skimpy swim-wear, college students sorted by major, class year, and tuition payment, men who had purchased fashion underwear, people who have lost loved ones, medical malpractice plaintiffs, people who have been arrested, high risk gamblers, and tenants who have sued landlords; the lists go on and on.[35] Even the list of lists available is voluminous. A marketing directory describes more than one thousand lists that can be purchased.[36] As one commentator noted, "the typical transaction between a merchant or seller and a consumer increasingly can be characterized as an exchange of goods or services for money and information."[37]

B. *Charitable Donor Lists*

Nonprofit corporations profit immensely from the sale and rental of donor's personal information. One estimate of the amount raised from this practice is between $800 million and $940 million yearly,[38] an amount intended as a "conservative one."[39] Obtaining lists can cost nonprofits between $65 and $125 per thousand names.[40] A list of 50,000 names is considered small.[41] As in

---

include terms giving consumers an opportunity to either opt-in or opt-out of secondary use of personal information); Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 2 (1996) (proposing federal statute granting individuals property rights in their electronic personas).

[35] *See* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1034 (1999).

[36] *See* 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).

[37] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2402 (1996).

[38] *See* Brock N. Meeks, Tough Love for Charity Data: Do-gooders Don't When They Shop for Your Privacy, *at* http://www.msnbc.com/news/6979654.asp (last visited April 13, 2002). This estimate consists of charities selling "housefile" databases containing lists of donors, their contact information, and the amount they previously donated.

[39] *Id.* The source of the estimate is a study by advocates who looked at the impact of possible new legislation that requires nonprofits to obtain prior approval before selling personal information, as this Article suggests.

[40] *See* Constance Casey, *The Doing Good Beat: Charities May Make More Money on Your Name Than on Your Check*, NEWHOUSE NEWS SERV., Oct. 5, 1999.

[41] *See id.* Interestingly, it is easier for an individual to gain access to a list of donors than it is for a shareholder to obtain a list of fellow shareholders under New York law. A shareholder

the consumer information trade, donor lists can contain names, addresses, telephone numbers, and details about the amount and frequency of donations.[42]

Nonprofits are not the only organizations that have access to many donor lists which nonprofit organizations and fundraising consultants purvey. If *any* individual expresses an interest, lists compiled from nonprofit sources are available for purchase through brokers or electronically.[43] Many nonprofits, however, keep their lists to themselves and barter them or sell them on an exclusive basis.

A driving force in the marketing practices of nonprofits is the highly competitive nature among these organizations for every donation. While the sale of donor lists raises high revenues, advocates of the practice argue that if list selling were prohibited, it would be difficult to start new charities without enormously high fundraising costs. Furthermore, an argument is made that list trading can help educate the public about the work being done by nonprofits in related fields. This argument is a tenuous justification, at best.

Some contend that when one gives a donation to a charity, the name and personal information that comes with the donation is more valuable than the donation itself.[44] Many fundraisers believe that direct mail via the sharing and renting of donor lists is essential to nonprofit fundraising.[45] Charities offer their donor lists to businesses looking for some of the forty million Americans who make purchases by mail or respond to contribution requests.[46] The growth of

---

who desires access to a shareholder list must be seeking access in the best interests of the corporation and not for his own personal motives. Corporations are permitted to deny a shareholder access to shareholder lists

> upon [the shareholder's] refusal to furnish to the corporation . . . an affidavit that such inspection is not desired for a purpose which is in the interest of a business or object other than the business of the corporation and that he has not within five years sold or offered for sale any list of shareholders of any corporation of any type or kind.

N.Y. BUS. CORP. § 624 (McKinney 2003). Similarly, under Delaware law stockholders have the right to inspect the list of the company's stockholders only for "a purpose reasonably related to the person's interest as a stockholder." DEL. CODE. ANN. tit. 8, § 220 (2003).

[42] *See* Anthony Giorgianni, *The Donor Name Game*, THE CHRON. OF PHILANTHROPY, Aug. 12, 1999, at 21.

[43] For instance, anyone with a credit card can go to www.richlists.com and purchase a list of donors who have contributed to Jewish, Catholic, children, cancer, and other nonprofit causes. Only $105 can get you 1000 donors who have given within ninety days of your list purchase. The Rich List company

> provides a number of related services to make your order a "one stop" call. The list representative will listen to your needs and suggest a list or maybe two. The company works with a printer and can help you develop graphics, and copy. Additionally, The Rich List can do merge purge, list cleaning & postal requirements, and manage your lists for rental. The Rich List can also do telethons, raise money, exchange lists and provide statistical studies.

The Rich List Company, What Does the Rich List Company Do?, *at* http://www.richlist.com/aboutrlc.htm (last visited Apr. 20, 2004). There are dozens of similar companies that aid and abet in the practice of cultivating, selling, and trading of donors' personal information.

[44] *See* Giorgianni, *supra* note 42.

[45] *See id.*

[46] *See id.*

the practice has nonprofits apprehensive about the possibility that their donors will learn about the list trade and be offended.

It is important to note that some charities assert that they never sell lists and that if they do engage in list sharing practices, they do so only with the express consent of their donors.[47] For instance, the American Heart Association (AHA) does not sell or trade its donor lists. Instead of selling, they rent their lists to other health related organizations on a one-time basis.[48] The AHA prominently asserts in its privacy policy that "[p]ermission is required before the AHA discloses personal information to a third party."[49] For these organizations, list selling or swapping can, potentially, undesirably discourage those who have made donations in the past.[50]

Other nonprofits defend the practice by stating their list practices are responsible.[51] Charities often refuse to sell their lists to groups whose material they deem to be objectionable or inappropriate.[52] Nonprofits often refuse to sell lists to competing organizations as well.[53] Additionally, charities often "seed" their lists with the personal information of people who work for the organization or are closely connected to it.[54] This practice enables the nonprofit groups to keep track of a how a list is being used and if the group that purchased the list has improperly used it.

It is well known that for-profit organizations consider the skillful exploitation of lists of prospective customers to be crucial to success in the world of retail business. It is less well known, however, that the intensive exploitation of lists of potential nonprofit charitable donors, subscribers, and

---

[47] *See, e.g.,* American Heart Association, Policy on Collection and Use of Personal Information, *at* http://www.americanheart.org/presenter.jhtml?identifier=11404 (last visited, Apr. 20, 2004).

[48] *See id.* For our purposes, renting the list for a one-time purpose is still exposing the personal information of charitable donors; therefore donors should be entitled to a clear and conspicuous right to refuse its privacy policy.

[49] *See id.*

[50] Indeed, there is a prevalent problem that the public's trust in nonprofits will diminish if they continue the nonconsensual use and dissemination of donors' personal information. A recent study conducted for the Better Business Bureau indicated that nine out of ten Americans "think it is *not* okay for a charity to raise money by selling donors' names and addresses to others." PRINCETON SURVEY RESEARCH ASSOCS., BBB WISE GIVING ALLIANCE DONOR EXPECTATIONS SURVEY: FINAL REPORT 7 (2001), *available at* http://www.give.org/news/Donor%20Expectations%20Survey.pdf. Moreover, "privacy concerns also rate as one of the two most important reasons why people are reluctant to make charitable contributions online." *Id.*

[51] *See* Giorgianni, *supra* note 42.

[52] *See id.*

[53] For instance, the Disabled American Veterans exchanges lists with many organizations, but not with other veterans groups. *See id.*

[54] *See* RIEVA LESONSKY, START YOUR OWN BUSINESS: THE ONLY START-UP BOOK YOU'LL EVER NEED (1998) (describing the list "seeding" process), *excerpted portion of book available at* http://www.entrepreneur.com/Magazines/MA_SegArticle/0,1539,265000----1-,00.html.

clients, is increasingly deemed indispensable to successful nonprofit revenue generation. A recent conference sponsored by the Direct Marketing Association, devoted to marketing by nonprofit organizations, emphasized the importance of mining data to nonprofit success. At the conference, several leaders of nonprofit organizations explained that the growth of their organizations could not have been accomplished as successfully without the skillful use of data collected by the organizations and of data rented, exchanged, or purchased from other nonprofits.[55]

III. CONCERNS ABOUT SHARING PERSONAL INFORMATION

Concern about excessive intrusions upon privacy resulting from the gathering of personal information by nongovernmental entities is nothing new.[56] As early as 1967, Professor Alan Westin issued a general warning about the impact on freedom of data collecting, trading and sharing.[57] As the practice has become commonplace, as the industry of data collection has grown, and as fundraising practices have become more and more sophisticated, American consumers have become increasingly concerned about their perceived loss of control over information.[58] The relatively young Internet medium in particular

---

[55] There were several panels discussing the detailed exchange in donor personal information including one devoted exclusively to donor list management. For information on the panels and issues discussed at the DMA sponsored nonprofit conference, see 2004 Washington Nonprofit Conference, Home Page, *at* http://dmany.convio.net/site/PageServer?pagename=homepage (last visited Aug. 4, 2003).

[56] *See* ALAN WESTIN, PRIVACY AND FREEDOM 33 (1967) ("In democratic societies there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth as a creature of God and a human being, and in the need to maintain social processes that safeguard his sacred individuality.").

[57] *Id.* An earlier warning was provided in *Olmstead v. United States*,

> Protection against such invasion of 'the sanctities of a man's home and the privacies of life' was provided in the Fourth and Fifth Amendments by specific language. But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> Moreover, 'in the application of a constitution, our contemplation cannot be only of what has been but of what may be.' The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.

277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting) (citations omitted).

[58] A Time/CNN poll found that ninety-three percent of Americans believe that "companies that sell information to others should be required by law to ask permission from individuals before making the information available." Richard Lacayo, *Nowhere to Hide*, TIME, Nov. 11, 1991, at 34. More recently, a PCWorld.com poll inquiring into privacy issues raised by the Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act, found that sixty-three percent were either very concerned or extremely concerned about having law enforcement scrutinize their Web habits. CNN.com, PC World Poll

has made the personal information struggle more difficult for privacy advocates, as it allows for easy access. For instance, with the click of a mouse, one can purchase lists of anti-gun control contributors, donors to causes that aid the mentally challenged, drug rehabilitation donors, ethnic contributors, humanitarian donors, and even "fat cats, who have previously contributed to both political parties."[59] There are literally dozens of websites that have complete lists of donor lists and their corresponding prices.[60] The lists go on and on, and their accessibility comes with little or no effort.[61]

A. *Intrusions and Inaccuracies*

Several obvious concerns center around violations of confidentiality that are inherent to the compilation of lists without the listed parties' knowledge or consent. While many organizations do indeed gather information with the consent of individuals, consent may be obtained with different degrees of meaningfulness and without providing specific knowledge of the purpose for which information will be used.[62] Individuals, furthermore, are frequently unaware of the myriad of organizations that collect personal information for commercial purposes without seeking consent.[63] Shadow groups and their surreptitiously gathered lists of personal information are particularly troubling. A related concern for consumers is the unnecessary or excessive acquisition of personal information. Information is often gathered "because it is there."[64]

Another important concern with the collection of personal information is accuracy.[65] The activity of collecting and disseminating information is inherently susceptible to error. Recording techniques, misleading information,

---

Highlights Privacy Concerns (2001), *at* http://www.cnn.com/2001/TECH/industry/10/08/privacy.poll.idg/index.html. For further discussion on the PATRIOT Act's relation to nonprofit context, see *infra* notes 176-85 and accompanying text.

[59] *See* W.S. Ponton, Inc., Philanthropic Donor Lists, *at* http://www.geocities.com/wsponton/pages/01philan (last visited Apr. 20, 2003).

[60] *See, e.g.*, The Rich List Company, Home Page, *at* http://www.richlist.com (last visited Apr. 20, 2004); USALists.com, Home Page, *at* http://www.USALISTS.com (last visited Apr. 20, 2004).

[61] *See supra* note 43 and accompanying text.

[62] For a discussion of meaningful consent in the context of patient privacy, see Helena Gail Rubinstein, *If I Am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate*, 25 AM. J.L. & MED. 203, 218 (1999) ("Without the ability to know and rely on uniform privacy regulations, patients may lack the basis for meaningful consent to disclosure of information. Lack of uniformity of privacy protections may adversely affect the integrity of health data and the quality of care itself by undermining efforts to automate health records.").

[63] *See generally* ERIK LARSON, THE NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES (1992).

[64] Reidenberg, *supra* note 36, at 203.

[65] *See* Organization for Economic Cooperation & Development: Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Mar. 1981, 20 I.L.M. 422 [hereinafter OECD Guidelines].

and incomplete collecting together contribute to accuracy concerns.[66] Additionally, the duration of storage of gathered information raises concerns.[67] Information may be stored beyond the life cycle of the purpose for which it was collected. Retention beyond such a time suggests that the information is being used for purposes other than were originally contemplated.[68] Moreover, as time goes by and the information ages, it may become obsolete or inaccurate.

B. *The Nonprofit Context*

Awareness of the problem of list sharing with special reference to nonprofit organizations has not been notable until recently. In particular, concerns have increased in the aftermath of September 11, 2001 when charitable organizations scrambled to collect funds aimed at assisting thousands of people who were deeply affected by the catastrophe.[69] Families of those who perished were typically designated as the intended recipients of extensive charitable campaigns—but there were reports of victims who did not receive any charitable assistance and reports of donors who wished to know where their donations were going but could not find out.[70]

---

[66] *See id.*

[67] *See id.*; *see also* Joel R. Reidenberg, *Multimedia as a New Challenge and Opportunity in Privacy: The Examples of Sound and Image Processing*, *at* http://www.datenschutz-berlin.de/infomat/heft22/teil2.htm (Apr. 20, 2004).

[68] *See id.*

[69] Notwithstanding the September 11 tragedy, New Yorkers donate over $10 billion to charity every year. *See* Office of New York State Attorney General, Charities, *at* http://www.oag.state.ny.us/charities/charities.html (last visited Apr. 20, 2004).

[70] *See Response by Charitable Organizations to the Recent Terrorist Attacks: Hearing Before the Subcomm. on Oversight of the House Comm. on Ways and Means*, 107th Cong. (2001) (statement of Daniel Borochoff, President, American Institute of Philanthropy). Indeed, Fox News' *The O'Reilly Factor* conducted a nightly segment interviewing executives from nonprofit charities as well as congressional leaders and victims in need. This news segment brought the importance of charitable accountability to the public perception. O'Reilly was also criticized for inaccurately accusing the United Way of diverting charity funds that were supposed to provide relief to September 11 victims. *See* Rational Radical, *Bill O'Reilly Is Guilty Once More of Sloppy, Misleading Journalism, This Time About the United Way* (2001), *at* http://www.therationalradical.com/dsep/bill-oreilly-united.htm. For more on the struggle of major charities in the aftermath of September 11, see David Barstow & Diana B. Henriques, *A Nation Challenged: The Charities; I.R.S. Makes an Exception on Terror Aid*, N.Y. TIMES, Nov. 17, 2001, at B1; David W. Chen, *A Nation Challenged: Charities; 9/11 Charities Set Cutoff Date For Applicants*, N.Y. TIMES, Feb. 15, 2002, at A1; Aaron Donovan, *Charity Donations in Month Long Campaign Total $35 Million*, N.Y. TIMES, Oct. 11, 2001, at B14; Daniel Henninger, *Wonder Land: Charity Begins at Home, Ends Up Nowhere*, WALL ST. J., Nov. 16, 2001, at A12; Diana B. Henriques, *Charity Overwhelmed in Bid to Meet Attack Victims' Bills*, N.Y. TIMES, Jan. 5, 2002, at A1; Stephanie Strom, *Families Fret As Charities Hold a Billion Dollars in 9/11 Aid*, N.Y. TIMES, Jun. 23, 2002, at A29. For a comprehensive discussion on all the legal issues arising out of the charity controversy resulting from the September 11 attacks including suggestions for how charities should handle future catastrophes, see Robert A. Katz, *A Pig in a Python: How the Charitable Response to September 11 Overwhelmed the Law of Disaster Relief*, 36 IND.

In an effort to better coordinate relief, representatives of the government forcefully urged charities to share lists of their program's benefit recipients with one another, and with the government, in order to diminish duplication and to avoid the further alienation of givers.[71] The focus of concern was on the sharing of lists of beneficiaries and not on the sharing of personal information about donors. Still, the suggestion that major charities should be pressured to share recipient lists, and that lists be shared without the consent of donors, has generated criticism of the way some nonprofit organizations handle their operational records and the information that they collect.[72]

C. *Voluntary Responses: Guidelines and Privacy Policies*

With the increased capabilities and actual practices of corporations in compiling lists containing personal information, privacy concerns have become important to consumers and charitable donors alike.[73] Marketing associations of nonprofit and for-profit vendors, Internet watchdog groups, and charitable solicitors have sought to address and allay these concerns through the development of voluntary standards and practices. This private approach exhorts organizations that gather personal information to develop, proclaim, and explain rules regarding their use of the information.

Given the degree to which the Internet has facilitated invasion of privacy, it is ironic but perhaps not surprising that Internet vendors and charitable solicitors have taken a more visible stand than conventional marketers with respect to their "privacy policies." Nearly every Internet website that solicits commercial transactions or nonprofit contributions posts a "privacy policy" somewhere. Privacy watchdog organizations and trade organizations, furthermore, have established minimum disclosure practices for sites that wish to advertise that their privacy policies are in compliance with watchdog or trade association rules.

Adherence by organizations to the stated policies of watchdogs and trade associations, however, has not been documented, and enforcement of the rules

---

L. REV. 251 (2003).

[71] *See* Diane Rezendes Khirallah, *Charities in Need of IT—Vendors Collaborate to Build a Central Database to Help Victims of the Sept. 11 Attack*, INFO. WK., Nov. 19, 2001, at 20; *see, e.g.*, Paulette V. Maehara, *Let Ethics Be Your Fundraising Guide*, 54 ASS'N MGMT. 30, 32 (2002).

[72] *See* Khirallah, *supra* note 71 ("The key issue here is whether the personal information about the recipients is used fairly." (quoting Jason Catlett, President of Junkbusters Corp., a privacy consulting firm)).

[73] Indeed, the dissemination of personal information has raised concerns about the prospect of identity theft. The FTC has indicated that identity theft is its number one source of consumer complaints. *See* Fed. Trade Comm'n, Identity Theft Complaint Data: Figures and Trends on Identity Theft, *at* http://www.consumer.gov/idtheft/ (last visited Apr. 20, 2004). For a comprehensive discussion of the privacy failures of regulators as a reason for increasing identity theft cases, see generally, SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY (2000).

that are established is sporadic. Some organizations with highly responsible Internet data collection policies, furthermore, have less responsible policies with respect to other types of transactions with their customers and donors.[74]

The policies themselves vary in the degree to which they tolerate collection and dissemination of information. Even the most ardent nonprofit privacy proponents rarely completely prohibit the sharing of personal information. The Privacy Rights Clearinghouse, a "nonprofit consumer education, research and advocacy program,"[75] for example, maintains a website that states in its own privacy policy that under no circumstance is the information it collects shared with third parties, but its policy does not prohibit sharing information within the organization.[76] The website of VolunteerMatch, a nonprofit organization that helps match nonprofit organizations with volunteers, on the other hand, needs to share the information it collects with others in order to pursue its mission. Its elaborate policy statement declares that while the privacy of website users is "important," the sharing of personal information is indispensable to its mission:

> Our ongoing commitment to the protection of your privacy is essential to maintaining the relationship of trust that exists between VolunteerMatch and all of our users . . . .
>
> This notice applies to all information you submit to VolunteerMatch, whether through the . . . Web site or through the Web site of one of our Partners. Please note that we cannot be responsible for the information you submit directly to third parties, including our Partners, who may have their own posted policies . . . . The types of personal information we collect are: For Newsletter Subscribers: First and Last Name, Email address; For Volunteers: First and Last Name, Email address, Phone number, ZIP code, Comments about opportunity optional; For Volunteers (with a personalized account): First and

---

[74] For instance, PC Connection, an Internet purveyor of computer and tech related goods maintains one privacy policy for its web consumers and one for its print catalog requests.

> When you visit our site: When you connect to our Web site, PC Connection's Web servers use non-persistent cookies to collect your IP address. Non-persistent cookies do not reveal your identity, they simply enable us to maintain custom settings and items in your shopping cart while you browse. The non-persistent cookie is temporarily stored to memory and is automatically discarded when you end your browser session.
>
> When you request a catalog: You are automatically placed on our mailing list when you submit a catalog request. In addition to receiving our catalogs, you may occasionally receive special mailings from us and/or from reputable companies whose products may be of interest to you.

PC Connection, Privacy Policy, *at* http://www.shop.pcconnection.com/Webcontent/Legal/PrivacyPolicy.htm (last visited Apr. 20, 2004). In the nonprofit arena, charities sometimes have privacy guidelines for those who visit their websites and separate privacy policies for those who donate funds. *See, e.g.*, Partners International Harvest of Hope, Security/Privacy Policy, *at* http://www.harvestofhope.org/index.cfm?FuseAction=Security (last visited Apr. 20, 2004).

[75] Privacy Rights Clearinghouse, Home Page, *at* http://www.privacyrights.com (last visited Apr. 20, 2004).

[76] Privacy Rights Clearinghouse, Privacy Policy, *at* http://www.privacyrights.com/policy.htm (last visited Apr. 20, 2004).

> Last Name, Email address, Phone number, ZIP code, Comments about opportunity (optional, Username and Password, Referral history, Customized email preferences (optional), Resume; For Nonprofit Organizations: Administrator information: First and last name, email, telephone number, ZIP code, username and password. Organization Information: Name of organization, contact information (including contact title, first and last name, phone, street address and email), EIN/tax identification number, mission statement, description of services, and minimum one category. Fax, web site address, and directions to physical location optional. Opportunity Information: Opportunity title, contact email, description, minimum one category and location information. . . . Required skills, date, time, commitment information and volunteer age/group size optional.
>
> How We Use Information: We use the Information we collect about you to facilitate the volunteering process and to provide information to you about VolunteerMatch and related industry topics. We use return email addresses to answer the email we receive. Please be aware that, to the extent required to provide our services, we share your Information with volunteers, nonprofit organizations, or our Partners, as applicable. For Newsletter Subscribers: . . We do not, however, sell, rent or trade our volunteer, administrator, nonprofit, or general newsletter email addresses to outside parties . . . .
>
> Cookies: Cookies are tiny data files that Web sites commonly write to your hard drive when you visit them so that they can remember you when you visit. A cookie file contains information that can identify you anonymously and maintain your account's privacy. Our site uses cookies to maintain a user's identity between sessions so that the site can be personalized based on user preferences or a user's history.[77]

Although the above policy indicates that personal information is not sold, there are no limits upon who the nonprofit chooses as its partners or the fees that the nonprofit may obtain by sharing with partners; nor are there limits on the use the nonprofit or its partners may make of the information they collect.

Current voluntary approaches made by for-profit and nonprofit marketers, in sum, have had a marginal impact on public awareness that information is collected by marketers, but they have not been proven effective at disclosing or restricting the concrete use being made of information.

IV. DONORS CONSIDERED AS CONSUMERS

The theory of the nonprofit corporation has difficulty incorporating the proposition that donors should be considered consumers. After all, the typical definition of a consumer transaction is one made for household or family purposes. Donors, however, are typically defined as persons who make gifts for the benefit of others rather than exchange transactions made in their self-

---

[77] VolunteerMatch, Privacy Policy, *at* http://www.volunteermatch.org/about/legal/privacy.jsp (last visited Apr. 20, 2004).

interest.[78] In the context of privacy protection, however, the strong similarities, characteristics, and intentions charitable donors and consumers collectively share, warrant their equivalence in legal terms in that context.

A. *Theoretical Considerations*

Charitable donors may have varying and unidentifiable reasons for donating money to charities.[79] First and foremost, however, donors want their donations to be utilized for the purpose that the charity purports that it will be used.[80] Additionally, most donors prefer that the charitable goal be accomplished at the lowest possible cost.[81] Notwithstanding the compelling fact that donors may have ulterior motives,[82] these descriptions firmly resemble consumer characteristics. Like donors, consumers want the goods and services they purchase to conform to their expectations and purported uses. Consumers also desire to acquire goods or services at the lowest possible costs.[83]

Furthermore, donors and consumers both face similar problems in addressing grievances that surface through their transactions. Donors and consumers are plagued by the problem of standing. Their right to sue is limited in most respects. This results from the judiciary's unwillingness to recognize the right to a citizen's suit when the attorney general is in a position to bring a suit.[84] The general rights of both classes are poorly defined, and both groups

---

[78] Section1.170A-13(c)(7)(iv) of the Income Tax Regulations defines donor as "a person or entity . . . that makes a charitable contribution of property." 26 C.F.R. § 1.170A-13(c)(7)(iv) (2004). There are many consequences beyond tax consequences, of course, which flow from designating a transfer as a donation rather than as a sale. Courts have defined the essence of a donation as an act of charity without consideration. In *Jacobs v. North Jersey Blood Center*, for example, the court asked, "what is a charity?" 411 A.2d 210, 211 (N.J. Super. Ct. Law Div. 1979). The court in *Ballentine v. Ballentine* said that a "charity, in its legal sense, may be more fully defined as a gift . . " 123 N.J. Eq. 577, 578 (N.J. 1938). A gift in common parlance means to give or donate something to someone "for free." Webster's Dictionary defines a "charity" as "an organization or institution engaged in the *free assistance* of the poor, the suffering or the distressed" WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 378 (4th ed. unabridged 1976) (emphasis added). Implicit in these definitions of charity is the concept that the donor may not "expect or receive anything of value in return for the gift or assistance given." *Id.*

[79] *See* Robert A. Katz, *Can Principal-Agent Models Help Explain Charitable Gifts and Organizations?*, 2000 WIS. L. REV. 1 (2000); *see also* Geoffrey A. Manne, *Agency Costs and the Oversight of Charitable Organizations*, 1999 WIS. L. REV. 227 (1999).

[80] *See* Manne, *supra* note 79, at 234.

[81] *See id.*

[82] It may be to the benefit of charitable donors to donate money to a charity, regardless of how efficiently the money is being used. A public showing of charity, tax benefits, or an altruistic urge to donate may be what is sought by the donor. *See id.*

[83] *But cf.* Katz, *supra* note 79 (arguing that charitable donors do not consume or purchase goods).

[84] *See* Manne, *supra* note 79, at 234; *see also* NORMAN I. SILBER, A CORPORATE FORM OF FREEDOM: THE EMERGENCE OF THE NONPROFIT SECTOR 1-14 (2001).

are confronted with difficulties in monitoring the acts of private enterprises.[85] Indeed, defining donors as consumers for the purposes of consumer protection legislation would grant private rights of action in many cases where standing to sue would be unavailable.

The similarities that can be inferred from the actions of both consumers and donors, along with the difficulties both contingents face, indicate the need for reform at the federal level. Moreover, if the federal government wishes to promote giving and robust growth in charitable contributions, charitable donors probably should be protected more than consumers with respect to the placement of their personal information on donor lists.

B. *Decisions Addressing the Donor/Consumer Distinction*

Few cases rationalize the distinction between consumers and donors that have been implied by the language of the statutory provisions. One FTC case, however, *In re El Paso Energy*,[86] touches on this distinction in dicta. In analyzing certain misrepresentations that occurred during the course of a charitable solicitation, the court remarked on the likeness and differences of consumers and charitable donors.

The FTC ruling emphatically proclaimed that there are "substantial differences between selling goods and services and seeking charitable donations."[87] The authority for this notion was the Supreme Court's treatment of charitable solicitation under the First Amendment. Citing *Village of Schaumberg v. Citizens for a Better Environment*,[88] which invalidated charitable solicitation rules that might have otherwise passed muster if only the regulation of commercial speech were involved,[89] the FTC concluded that the

---

[85] *See* Manne, *supra* note 79, at 228.

[86] No. C-3997, 2001 F.T.C. LEXIS 8 (F.T.C. Jan. 30, 2001).

[87] *Id.* at *12.

[88] 444 U.S. 620 (1980).

[89] As Justice White stated,

> [C]haritable appeals for funds, on the street or door to door, involve a variety of speech interests . . . that are within the protection of the First Amendment . . . . Soliciting financial support is undoubtedly subject to reasonable regulation but the latter must be undertaken with due regard for the reality that solicitation is characteristically intertwined with informative and perhaps persuasive speech seeking support for particular causes or for particular views on economic, political or social issues, and for the reality that without solicitation the flow of such information and advocacy would likely cease . . . .

Id. Along the same lines, see *Secretary of Maryland v. Joseph H. Munson Co.*, 467 U.S. 947, 962 (1984), which held that charitable fundraising constitutes speech under the First Amendment.

These holdings are distinguishable from the donor list context. In the donor list context, charities are misappropriating the donor's personal information rather than engaging in door-to-door solicitation in furtherance of their message. The latter inherently provokes First Amendment protections while the former has no relationship with First Amendment activity. Recently, the Supreme Court limited *Schaumberg*'s application to charitable solicitation. Where the solicitation is false, misleading, or is not related to First Amendment activity, the

sale of goods and services are often subject to separate statutory and regulatory schemes, and are therefore "different forms of activity."[90]

The FTC's analysis is inapplicable to the context of nonconsensual selling of donor lists. Whether the personal information in a list was acquired in connection with a gift or a purchase, the most salient fact is that information obtained by either a seller or a donee may have been obtained with an expectation that it would be be kept private. Given the purposes the FTC should be protecting, namely, the rights of individuals to be free from "deceptive" or "unfair" practices, donors and consumers alike both face virtually identical problems with respect to the issue of informational privacy.[91]

C. *Weighing Consumer and Donor Interests in List Sharing*

As a group, consumers have reasons not only to be concerned about the information trade, but also to welcome benefits from it. Many consumers make purchases in response to mailings, online offerings, and telephone solicitations.[92] Consumers who transact in these ways benefit when merchants correctly identify their interests. For instance, major computer catalog sellers often send unsolicited e-mails to individuals who they have reason to believe may be interested in purchasing computers. Would-be purchasers need look no further than their e-mail inbox for a favorable deal. An e-mail of this sort can save the consumer time and money by lowering search costs, as the consumer will not have to travel to a computer vendor.[93] Proponents of a broad and permissive trade in information argue that benefits to potentially interested consumers outweigh impositions on uninterested consumers.[94]

---

solicitation is not "place[d] under the First Amendment's cover." Illinois *ex rel.* Madigan v. Telemarketing Assocs., 123 S. Ct. 1829, 1831 (2003).

[90] *In re El Paso*, No. C-3997, 2001 F.T.C. LEXIS 8, at *12.

[91] Recently, in *Madigan v. Telemarketing Associates, Inc.*, 123 S. Ct. 1829 (2003), in a case involving fraudulent misrepresentation of charitable funds, the Supreme Court's analysis suggests that the Court may consider regulatory actions in the area of misrepresentation to donors more favorably. Along these lines, the Court upheld the government's right to "vigorously enforce antifraud laws to prohibit professional fundraisers from obtaining money on false pretenses or by making false statements." *Id.* at 1839. Moreover, the Court upheld the right of states to "maintain fraud actions when fundraisers make false and misleading representations designed to deceive donors about how their donations will be used." *Id* at 1843.

[92] *See* Bibas, *supra* note 34, at 599 ("Many consumers enjoy receiving mailings and shopping at home.").

[93] *See* 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.").

[94] *See, e.g., Information Privacy: Hearing Before the House Subcomm. on Commerce, Trade and Consumer Protection*, 107th Cong. (2001) (statement of Jerry Cerasale, Senior Vice President, Government Affairs, Direct Marketing Association, Inc.) (arguing that companies can effectively address and protect consumer privacy), *available at* http://energycommerce.

D. *The Virtues of Consumer Profiling*

It has been argued that the greater availability of information about consumers actually reduces the quantity of junk mail. The more sellers and merchants learn about consumers, this argument goes, the better refined their marketing and solicitation efforts will be.[95] Subsequently, as a result of narrower target marketing schemes, unwanted solicitations will be reduced. If sellers are not allowed to create consumer profiles, they may respond by soliciting all consumers.

As states consider limits on the trade of personal information, lobbyists have pursued this line of argument forcefully. Several states have recently considered enacting privacy rules that would restrict the construction of profiles without consumer consent, and which would be tougher than those at the federal level.[96] Vermont, New Mexico, and California are moving ahead with tougher financial privacy rules.[97] Lobbyists who represent the financial and

---

house.gov/107/hearings/06212001Hearing292/Cerasale464.htm.

[95] *See* Dee Prigden, *How Will Consumers be Protected on the Information Superhighway?* 32 LAND & WATER L. REV. 237, 240 (1997); *see also Statement of the Federal Trade Commission on "Online Profiling: Benefits and Concerns" Before the Senate Comm. on Commerce, Science and Transportation*, 107th Cong. (2000) (remarks of Jodie Bernstein, Director, Bureau of Consumer Protection), *available at* http://www.ftc.gov/os/2000/06/onlineprofile.htm. *But cf.* FED. TRADE COMM'N, PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY SESSION THREE: CONSUMER ONLINE PRIVACY, VOLUME 3 (1997), *available at* www.ftc.gov/bcp/privacy/wkshp97/volume3.pdf (quoting Jason Catlett, Chief Executive Officer, Junkbusters Corp., who states that ten thousand pieces of spam cost one dollar to send).

[96] *See* Russell Gold, *States Mull Opt-In, Opt-Out Rules*, WALL ST. J., Mar. 13, 2002, at B8.

[97] *See id.* Recently, a California state senator's attempt to expand financial privacy was blocked in the California state assembly. Constituents are currently attempting to pass the bill into law via popular initiative in March 2004. *See* Steve Geissinger, *Lawmakers Kill Speier's Financial-Privacy Bill; Supporters Say They Will Take Fight to the Ballot Box*, SAN MATEO COUNTY TIMES, July 9, 2003; Carolyn Said, *Privacy Bill Backers Ready to Go to Ballot: Pass Law or Face Initiative, They Tell Legislature*, SAN FRAN. CHRON., July 31, 2003, at A1. The initiative calls for a complete "opt-in" requiring banks to procure permission from consumers before disseminating their personal information to telemarketers and the like. *See* Editorial, *Privacy Revolution is Here*, SAN FRAN. CHRON., July 31, 2003, at A20.

As of February 25, 2002, the New Mexico Statutes were amended, granting individuals greater protection of their nonpublic personal health information and personal financial information. N.M. STAT. ANN. § 13-1-3 (Michie 2003), *available at* http://www.insurcompweek.com/pdf/0114_nm_privacy_regs.pdf. The new laws were intended to afford individuals greater privacy protections than those provided in the Gramm-Leach-Bliley Act, 15 U.S.C. § 6716 (2000). Vermont also followed through by passing similar opt-in requirements that have insurance and financial services corporations scrambling to comply. Prudential Securities was forced to add the following footnotes to its national general notice to comply with the Vermont opt-in requirement: "We will not disclose information about our Vermont customers and former customers to non-Prudential businesses for their use in offering their products or services to you." Privacy Regulation Report, 2002 Privacy Notice Survey: Custom Preferences & State Requirements Drive Change, *at* http://www.privacyregulation.com/jsp/article.jsp?article_id=26839 (last visited Aug. 5,

insurance industries have argued that tougher privacy rules will inevitably stop the flow of efficient marketing.[98] They further assert that "if [companies] can't use customer data to target their advertising, [they will resort] to more mass mailings and telemarketing."[99] Ultimately they suggest that privacy laws do not stop marketing.[100]

These arguments have been criticized by privacy advocates who counter that if less privacy actually benefited consumers by reducing their junk mail, consumers would, if given a choice, choose to surrender their privacy.[101] Furthermore, the industry's argument against limits assumes that businesses would not respond to the loss of information by implementing a more cost-efficient alternative to direct solicitation efforts.[102] The ultimate fallacy of this argument is that it presupposes that alternate methods of reducing unwanted solicitations cannot be devised.[103]

The dissemination of personal consumer information via computer databases theoretically makes it possible to sell products at lower prices.[104] If the cheapest way for a seller to market products is by utilizing a computer database, this decreases the marketing costs of the seller, which theoretically will decrease the costs for consumers.[105] Indeed, the return for direct mail advertising is asserted to be more than twice that of more expensive television commercials.[106] If sellers were required to market to consumers only by using

---

2003).

[98] *See* Gold, *supra* note 96.

[99] *Id.*

[100] *See id.*

[101] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1217-18 (1998).

[102] *See* Sovern, *supra* note 35, at 1050.

[103] *See id.*

[104] *See, e.g.*, David 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 profile lists, because they send fewer mail advertisements, and they send them only to those persons who are likely to purchase the product.").

[105] *See id.* In the alternative, Ian Ayres and Matthew Funk recently recommended economic disincentives to telemarketing invasions of privacy:

> [W]e would require ... standardized, initial disclosure that a call is an unsolicited telemarketing call and the amount of per-minute compensation .... The intermediaries could also play a roll in verifying to the consumer that a particular telemarketing call was in fact paying compensation .... Indeed, far from the status quo, a telemarketer-choice regime with automated filtering by households is likely to be largely equivalent to a household-choice regime with automated filtering by telemarketers .... Each month's phone bill will disclose the telemarketing credits that the household receives (and might disclose how the consumer could vary the default price).

Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77, 112-16 (2003). We will discuss this "market theory of privacy" and the accompanying economic disincentives as applied to the nonprofit context *infra* at Part VII.

[106] *See* Susan Headden, *The Junk Mail Deluge*, U.S. NEWS & WORLD REP., Dec. 8, 1997, at 42 (stating that ten dollars is generated for every one dollar spent on direct mail advertising). The average mailing generates ten times the response produced by a newspaper

expensive means of communication such as television, radio, and newspaper advertising, sellers would have to increase the price of the products or forgo selling the products altogether.[107] Consumers may also benefit from a potential lender's access to financial information because a lender's ability to determine a consumer's creditworthiness allows the lender to customize interest rates on loans.[108]

Although not a benefit to consumers, there is another interest that should be factored into any analysis of the appropriate restrictions on marketing and list sharing in the interest of privacy rights. Sellers have a legitimate interest in being able to inquire about all aspects of the sales environment in which they operate. The interest of companies in gathering information about the tastes and preferences of consumers is crucial in their ultimate quest for maximizing future streams of revenue.[109]

Ultimately, sellers seek personal information about potential buyers as part of their own solicitation efforts.[110] The compilation and sale of lists is big business, and yet the costs associated with this business are low. Once a list exists the cost of maintaining it is relatively inexpensive.[111] Some companies earn more from selling customer lists and profiles than selling their own goods and services.[112] Indeed, some companies are pursued by merger partners because of the quality and quantity of their lists.[113]

In sum, the benefits of the information trade to sellers are tremendous. A 1996 Gallup poll found that seventy-seven percent of companies use marketing techniques that involve consumer lists and target marketing.[114] The total amount spent on mailing lists in this country is staggeringly approximated at $3

---

advertisement and one hundred times the response from a television commercial. *See* Jim Smolowe, *Read This!!!!!!!!*, TIME, Nov. 26, 1990, at 65.

[107] Additionally, Stephen Bibas claims that mail order selling reduces damage to the environment because it enables people to shop without traveling. *See* Bibas *supra* note 34, at 600. *But cf.*, Smolowe, *supra* note 106.

[108] *See* Judith B. Prowda, *Report: A Lawyer's Ramble Down the Information Superhighway: Privacy and Security of Data*, 64 FORDHAM L. REV. 738, 751 (1995) (noting claims of consumer benefits based on wide dissemination of personal information).

[109] *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, 88 (1996) (comparing the relationship of sellers and buyers to that of anglers and trout).

[110] *See id.*

[111] *See* Karlene Lukovitz, *Cashing in on Renting Your Lists*, FOLIO, Oct. 1985, at 106.

[112] *See* Headden, *supra* note 106, at 45; *see also* Smolowe, *supra* note 106.

[113] *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 336-37 (1996) (stating that pharmaceutical company merged with mail-order pharmacy to obtain the latter's detailed personal information records. Additionally, a prescription drug benefits plan manager sought to purchase a corporation that maintained a prescription drug database and owned two pharmacies).

[114] *See* BD. OF GOVERNORS OF THE FED. RESERVE SYS., REPORT TO CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION & FINANCIAL FRAUD 7 (1997), *available at* http://www.federalreserve.gov/boarddocs/rptcongress/privacy.pdf.

billion per year.[115] According to one estimate, consumer list direct marketing potentially generated $30 billion in sales by the end of the 2002 fiscal year.[116] The industry of compiling consumer and donor lists and profiles employs more than eighteen million people,[117] and the business is growing at a pace estimated at twice that of the United States' gross domestic product.[118]

Trade of information does have certain undeniable benefits, but those benefits are asymmetrically distributed toward sellers and toward those who are interested in receiving unsolicited marketing appeals. These benefits do foster a more efficient relationship between consumers and sellers, but the extent of the benefits should not be exaggerated.

E. *Virtues in the Nonprofit Context*

The detriments resulting from the dissemination of charitable donor lists are apparent. The donor, who by virtue of her donation injects her personal information into the stream of commerce, is continually harassed by companies and organizations that receive her information without her consent. This is essentially the identical problem that consumers are confronted with. Some charities have justified the practice on the theory that if donors contribute to one charitable organization, they will not mind being solicited by another.

Just as the sale of information has its benefits for consumers, the formulation of a donor database or list, and its subsequent sale or rental, has purported benefits as well. As mentioned, the donor lists give charities the ability to market their causes and pour in revenues. Indeed, there are often charitable donors who donate to fixed charities on a monthly or yearly basis. The charities may give donors the opportunity to give to similar causes that donors may indeed want to know about. Nonprofits feel that making the lists available to one another is an essential transaction that allows them to find people who are most likely to give.[119]

Additionally, if charities are able to use donor lists in efficient marketing, a greater amount of money can theoretically be used to help people actually in need. In this respect, such marketing may actually be beneficial.

---

[115] *See* Fenrich, *supra* note 33, at 956.

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

[117] *See* Fenrich, *supra* note 33, at 956.

[118] *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").

[119] *See* Giorgianni, *supra* note 42, at 21.

V. GOVERNMENT RESPONSES

In the United States, the right of nongovernmental entities to compile and distribute personal information is broadly established.[120] Not only are there acknowledged benefits to the aggregation of personal information about consumers for marketing purposes,[121] but there is also, as a general matter, no right to control the private use of personal information that is outside one's own possession.[122]

The importance of privacy concerns, however, in combination with the inadequacy of voluntary approaches, has provoked government regulation of certain types of information gathering and list-sharing activities. On the commercial side, the sale of personal information that is gathered in connection with commercial transactions has been restricted through the establishment of certain rules aimed at promoting accuracy, preventing discrimination, diminishing harassment, and preserving the confidentiality of certain types of records.

A. *Individualized Regulatory Constraints*

In the words of Professor Joel Reidenberg, "the American legal system

---

[120] *See, e.g., In re* Doubleclick Privacy Litig., 154 F.Supp.2d 497 (S.D.N.Y. 2001) (dismissing a complaint alleging the nonconsensual collection of personal information). In *Doubleclick*, the court emphatically stated "although demographic information is valued highly . . . the value of its collection has never been considered a economic loss to the subject." *Id.* at 525; *see also* Tarver v. Smith, 402 U.S. 1000, 1000 (1971) (Douglas, J., dissenting) (stating that "[t]he ability of the Government and private agencies to gather, retain, and catalogue information on anyone for their unfettered use raises problems concerning the privacy and dignity of individuals."); McNally v. Pulitzer Publ'g Co., 532 F.2d 69, 76 (8th Cir. 1976) (holding that *only* the most intimate aspects of people's lives have been held to be constitutionally protected); Fenrich, *supra* note 33; Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395 (1987); Marsha Cope Huie et al., *The Right To Privacy In Personal Data: The EU Prods The U.S. And Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391 (2002); Tracie B. Loring, Comment, *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421 (2002).

Additionally, it should be noted here that the European Union and the United States drastically differ in the regulation of privacy and personal information. While the United States has enacted piecemeal legislation, the European Union countries have adopted a comprehensive directive. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 seeks to offer broad protections to individuals with regard to the processing of personal data and on the free movement of such data. The Directive went into effect in 1998. EU Directive 95/46/EC of 24 October, 1995, *reprinted in* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 213-46 app. A (1998).

[121] *See supra* notes 95-118 and accompanying text.

[122] *See* Joel Reidenberg et al., *Panel III: The Privacy Debate: To What Extent Should Traditionally "Private" Communications Remain Private on the Internet?*, 5 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 329, 333 (1995).

responds incoherently and incompletely to the privacy issues raised by existing information processing activities in the business community."[123] The most significant legal rules at the federal level are in the areas of video and cable privacy, consumer medical records, children's online privacy, and bank and financial records.[124] Congressional activity with regard to personal information protection has been largely reactive, targeting industries on a case-by-case basis, and often responding after extreme instances of privacy infringement.[125] Congress recently has recognized a need to explore the possibility of further regulation of personal information gathering practices by for-profit entities.[126] It has refused, however, to create a coherent response based on fundamental principles and policies. Consequently, while some personal information cannot be sold, most commercial uses for personal information are not regulated at all, and the problem of donor privacy has, except for recent security provisions of the USA PATRIOT Act, ignored charitable donors entirely.[127]

Former Vice President Al Gore expressed his view of the problem during the last election: "We live," he said, "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."[128] This observation is still accurate.

1. *Video and cable privacy.*

The regulation Al Gore was speaking of involves the home entertainment industry.[129] The Video Privacy Protection Act prohibits the disclosure of titles of particular videos rented by any customer. However, the law does permit disclosure of customer names and addresses as well as subject matter interest

---

[123] Reidenberg, *supra* note 36, at 199.

[124] *See* Sovern, *supra* note 29, at 1306.

[125] *See* Reidenberg, *supra* note 36, at 209 (describing the "mosaic" approach to privacy concerns that responds to narrow problems).

[126] Representative Billy Tauzin (R.-La.), who chairs the full Committee on Energy and Commerce, cited "a need to explore additional legislative efforts that will address an apparent failure in the marketplace to protect consumers' privacy." *Challenges Facing the Federal Trade Commission Before the House Subcomm. on Commerce, Trade and Consumer Prot.*, 107th Cong. (2001) (statement of Rep. Billy Tauzin, Chair, House Comm. on Energy and Commerce), *available* at http://energycommerce.house.gov/107/Hearings/11072001hearing403/The_Honorable_Billy Tauzin.htm.

[127] For a more plenary discussion on the USA PATRIOT Act in this context, see *infra* notes 176-85 and accompanying text.

[128] Sheryl G. Stolberg, *Privacy Concerns Delay Medical IDs*, N.Y. TIMES, Aug. 1, 1998, at A10 (quoting Former Vice President Al Gore). Gore was referring to a federal statute that makes it illegal to disseminate information about what videos people rent. This statue will be discussed immediately *infra*.

[129] 18 U.S.C. §§ 2710-2711 (2000). The scope of § 2710 applies to consumers, and would not govern disclosing gifts of videotapes. "§2710. Wrongful disclosure of video tape rental or sale records. (a) Definitions. For purposes of this section—(1) the term 'consumer' means any renter, purchaser, or subscriber of goods or services from a video tape service provider." *Id.* § 2710.

for marketing purposes, provided that the consumer is given the option to opt-out of such an arrangement.[130] Civil remedies and statutory damages are available to aggrieved individuals.[131]

The Cable Communications Policy Act of 1988 similarly purports to address the problem of informational privacy where cable communications media are involved.[132] Subscriber information and viewing habits may be disclosed to third parties only with the subscriber's consent or for a legitimate business activity related to the service.[133] A mailing list can be disseminated if each subscriber has an opportunity to opt-out.[134] These statutes demonstrate the industry-specific nature of the federal government's response to consumer privacy concerns.

2. *Consumer medical records.*

The Clinton Administration's Department of Health and Human Services attempted to develop privacy regulations as required by the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[135] Indeed one of the delineated purposes of HIPAA was "to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information."[136] Generally, healthcare consumers are able to require healthcare institutions to give patients

---

[130] *See id.* § 2710(b)(2)(D)(i)-(ii).

[131] *See id.* § 2710(c).

[132] 47 U.S.C. § 551(b) (2000). The privacy related subsections of the statute provide, in relevant part, that:

> (1) a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.
>
> (2) A cable operator may use the cable system to collect such information in order to
>
> (A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or
>
> (B) detect unauthorized reception of cable communications. . . . .
>
> . . .
>
> (c)(1) a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.

Id.

[133] *Id.* § 551(b)(1).

[134] *Id.* § 551(c)(2)(C).

[135] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.).

[136] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164). Among the other purposes of the Act are "to improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care" and "to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals." *Id.*

notice of their information practices, and enable individuals to gain access to their own medical records.[137] The privacy standards apply to "covered entities" that are identified as "health care providers," "health plans," and "health care clearinghouses."[138] Patients who receive services at both nonprofit and for-profit health care providers are covered by the Act, although the personal information that health care providers collect from donors is not protected.

The HIPAA privacy standards purport to create a national framework for health privacy protection to enhance the protection of patient medical and "protected health information."[139] The privacy standards regulate the internal use and external disclosure of health information and medical records.[140] Included are new special rules for obtaining patient consent and authorization to use and disclose medical information.[141] Additionally, individual patients will have the right to inspect or obtain records of their own healthcare information and amend any inaccurate information.[142] Further, patients will have the opportunity to request a restriction of the use or disclosure of their records for treatment, payment, and health care operations, and to receive notice of a health care provider's privacy practices.[143] These privacy measures

---

[137] *See id.* While most Americans deem their medical information to be most sensitive, this information is widely available. *See* Robert W. Woody, *Health Information Privacy: The Rules Get Tougher*, 8 CONN. INS. L.J. 211, 213 (2001-2002). Unfortunately the noble Hippocratic oath is mere ideology. The oath reads as follows: "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick or even apart therefrom, which ought not be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets." *available at* http://www.epic.org/privacy/medical/.

[138] 45 C.F.R. § 164.104 (2004). The definitions of these terms as provided in the Act are of significant importance.

[139] What medical information is subject to the Act has been an increasingly complex inquiry.

> 'Health information' includes any oral or recorded information that is created or received by a covered entity or certain other entities and that relates to the past, present, or future: (1) physical or mental health or condition of an individual and the provision of health care to an individual; or (2) payment for the provision of health care to an individual. 'Protected health information' is that subset of health information to which the rules' restrictions on use and disclosure apply. Protected health information is: (1) 'individually identifiable health information' that is transmitted or maintained in electronic media or in any other form or medium. 'Individually identifiable health information' is health information that identifies an individual or that can be used to identify the individual (including demographic information). Protected health information does not include health information contained in certain education records and student medical records.

Woody, *supra* note 137, at 220 (citations omitted).

[140] Another healthcare privacy issue is genetic profiling. The use of genetic data to discriminate in both employment and health insurance is troubling to lawmakers, consumers, and healthcare professionals, alike. For a discussion of potential problems with genetic profiling and an example of how a railroad company used the procedure to asses the viability of medical claims by its employees, see Dana Hawkins, *The Dark Side of Genetic Testing*, U.S. NEWS & WORLD REPORT, Feb. 19, 2001, at 30.

[141] It is important to note that the consent requirement may be removed due to current proposed changes to the regulations.

[142] *See* 45 C.F.R. § 164.520 (2004).

[143] *See* 45 C.F.R. § 164.502 (2004).

were effective as of April 2003.[144]

While HIPAA seems like a major shift towards protecting the private information of healthcare consumers, it has several significant shortcomings. The Act allows researchers and public authorities to access protected health information without patient authorization and consent.[145] This has led commentators and privacy advocates to believe that there is a significant chance for challenges invoking the Fourth Amendment privacy rights of patients.[146] Additionally, while the rules create an administrative enforcement mechanism, they do not create a federal private cause of action for individuals who are injured by a violation of the rules.

Lastly, and perhaps most importantly, the limitation of coverage to specifically enumerated "covered entities" shields many entities that have had a field day in disseminating personal information.[147] For instance, "Business Associates" of covered entities—businesses that provide administrative, management, legal, accounting, and other oversight services to healthcare providers and health plans—would not be subject to legal sanction.[148] This is troubling because these precise associates are the ones who are mostly responsible for the dissemination of medical information without patient consent. Thus, while HIPAA does afford consumers some protections, it falls short of taking a significant step to protect the private medical information of patients.[149]

3. *Children's privacy online.*

Children have become increasingly vulnerable to privacy threats, particularly with their increased use of the Internet. In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA),[150] which regulates

---

[144] *See* Andrew S. Krulwich & Bruce L. McDonald, *The Vulnerability of HIPAA Regulations to First and Fourth Amendment Attack: An Addendum to "Evolving Constitutional Privacy Doctrines Affecting Healthcare Enterprises,"* 56 FOOD DRUG L.J. 281, 282 (2001).

[145] *See* 45 C.F.R. § 164.512 (2004).

[146] *See* Krulwich & McDonald, *supra* note 144, at 303 (arguing that "[t]he provisions allowing release of protected health information without the individual's authorization to government officials for law enforcement, public health, and research purposes do not take into account the individual patient's Fourth Amendment rights to protect medical information . . .").

[147] For a more comprehensive discussion of the Act's shortcomings in these respects, see generally, Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 619 (2002).

[148] *See* Laura Landro, *Health-Privacy Act Poses Problems*, WALL ST. J., Apr. 24, 2003, at D3.

[149] *But cf.* Susan M. Gordon, *Privacy Standards of Health Information: The Misnomer of Administrative Simplification*, 5 DEL. L. REV. 23, 56 (2002) (arguing that the "privacy regulations will do much to improve the confidentiality of medical records").

[150] 15 U.S.C. § 6501 (2000).

online information collected from children less than thirteen years of age.[151] Congress was prompted to regulate this information because young children are unaware of the privacy risks involved in revealing personal information and Internet websites were actively collecting data from web surfers.[152] The Act is designed to stop unfair and deceptive acts and practices involving the disclosure and collection of personal information by and from young children.[153]

The Act is broad in scope, applying to "any person who operates a website [sic] located on the Internet or an online service and who collects or maintains personal information from or about the users . . . where such website or online service is operated for commercial purposes . . . ."[154] The Act requires parental permission before a website can gather a child's personal information. Further, the Act includes mechanisms for controlling access to personal information and enforcing its proper use. The FTC is empowered to implement and enforce COPPA by its Section Five jurisdiction.[155] In addition, § 6504 of COPPA authorizes state attorneys general to enforce compliance by filing actions in federal court after giving the FTC prior written notice.[156]

COPPA requires that a website obtain "verifiable parental consent" before collecting information from a child.[157] To obtain verifiable parental consent, a website operator must make:

> [A]ny reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal

---

[151] *See id.* Pursuant to COPPA, the FTC issued a rule implementing the requirements of the legislation. *See* 16 C.F.R. § 312.1 (2004). For an in-depth discussion of the Act, see generally, Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 HOUS. L. REV. 751 (2001).

[152] The legislative history suggests that the purpose of the legislation was

> to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent.

144 CONG. REC. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan); *see also* Joe Salkowski, *Privacy-Protection Policy For Kids Can Benefit Adults*, CHI. TRIB., Nov. 1, 1999, at 2 (explaining benefits to adults of new child privacy regulations).

[153] *See generally* 144 CONG. REC. S11,657 (daily ed. Oct. 7, 1998) (statement of Sen. Bryan) (explaining goals and development of COPPA legislation).

[154] *See* COPPA, 15 U.S.C. § 6502(b)(1)(A)(i) (2000) (defining term "operator").

[155] For a discussion of Section Five jurisdiction of the FTC, see *infra* notes 203-09 and accompanying text.

[156] Another enforcement procedure is found in the safe harbor rules that subject participants to a yearly audit of their information practices. *See* 16 C.F.R. § 312.10 (2004).

[157] COPPA, 15 U.S.C. § 6501(2)(A) (2000).

> information and the subsequent use of that information before that information is collected from that child.[158]

Like the other federal legislation discussed in this Article, COPPA is inadequate in many respects. The Act only protects children under the age of thirteen and does not protect older youths that face similar privacy concerns and are certainly not apprised of information collection and its potential detriments. Furthermore, a child or parent who has been victimized does not benefit from a private right of action. Any regulation directed at protecting an individual's privacy rights should provide for an avenue of relief on behalf of the victim.[159] Most importantly, general adult websites do not have to comply with the Act unless they have actual knowledge that the online user is a child under the age of thirteen.[160]

Moreover, website operators have discovered ways to circumvent the Act. For instance, "[t]o verify that the parent is the one who has denied or given consent, some Web sites may choose to require credit card numbers or photocopies of driver's licenses."[161] Thus, the process of giving consent exposes the adult's personal information to gathering, which is currently not prohibited by law. Lastly, enforcement and detection of web operators who are in violation of COPPA is a mystery. A study examining the compliance of over 100 websites revealed that "a disturbingly large number of children's sites are still collecting personal information from children without providing notification of their privacy policies or obtaining parental permission."[162]

4. *Financial and credit information.*

Congress has targeted other industries with respect to the dissemination of

---

[158] *Id.* § 6501(9). Parental consent is not required when the website operator uses information to "respond directly on a one-time basis to a specific request from the child and is not used to re-contact the child" or when the request for information is needed "for the sole purpose of obtaining parental consent." *Id.* § 6502(b)(2)(A).

[159] *See* Nicholas W. Allard, *Privacy On-Line: Washington Report*, 20 HASTINGS COMM. & ENT. L.J. 511, 528 (1998) (highlighting recommendations of 1995 United States Information and Infrastructure Task Force); Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1223 (1997) (recommending elements of comprehensive privacy regulation system). For recent commentary addressing privacy rights under COPPA, see generally, Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6 (2000); Melanie L. Hersh, Note, *Is COPPA a Cop Out? The Child Online Privacy Protection Act as Proof that Parents, Not Government, Should be Protecting Children's Interests on the Internet*, 28 FORDHAM URB. L.J. 1831 (2001).

[160] *See* 16 C.F.R. § 312.3 (2004).

[161] Kalinda Basho, Comment, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507, 1520 (2000) (examining COPPA enforcement problems).

[162] *See* Net Family News, That Sticky Kids' Privacy Issue, *at* http://www.netfamilynews.org/sl990723.html (citing CENTER FOR MEDIA EDUCATION, CME ASSESSMENT OF DATA COLLECTION PRACTICES OF CHILDREN'S WEB SITES (1999)).

personal information. The Fair Credit Reporting Act[163] (FCRA), which targets the financial services industry, is widely acknowledged as inadequate.[164] Despite Congress's efforts "credit reporting agenc[ies] ha[ve] substantial latitude to disseminate regulated personal information without an individual's consent."[165] This bill was said to be "butchered" as a direct result of industry lobbying pressures.[166]

The FCRA purports to regulate the disclosure and collection of consumer credit information in personal transactions between consumers and credit providers, particularly the use of such information by "consumer reporting agencies."[167] Consumer reporting agencies are obligated to provide consumers with the opportunity to access and correct credit information, and FCRA imposes limitations on the use of consumer credit information and significant fines for noncompliance.[168] The Act was later amended to provide, *inter alia*, that a "consumer report" excludes the communication of consumer credit information to "affiliated" persons, provided that the credit provider "clearly and conspicuously" discloses to the consumer that such information will be communicated among affiliates.[169] Further, the consumer is required to be given the opportunity to opt-out of such disclosures.[170]

The Gramm-Leach-Bliley Act[171] (GLBA) similarly regulates financial information. The Act requires financial institutions to disclose their privacy policies to their customers. The policies generally contain the practices regarding the collection, use, and disclosure of customer information.[172] Further, the Act permits consumer information to be shared with third parties provided that the consumer receives notice from the financial institution and did not opt-out of such sharing.[173] Perhaps GLBA's most notable shortcoming is that it allows financial institutions to share nonpublic personal information with their affiliates.[174] In essence, the Act allows banks, credit card companies,

---

[163] 15 U.S.C. § 1681 (2000). The Act is limited to credit reporting organizations only, i.e., organizations that prepare and disseminate personal information in a consumer report bearing on an individual's credit-worthiness, credit standing, capacity, character, general reputation, personal characteristics, and mode of living. *Id.*

[164] *See* Reidenberg, *supra* note 36, at 210-14 (revealing the Act's shortcomings with respect to dissemination of consumer information).

[165] *Id.* at 212.

[166] *See* Bibas, *supra* note 34, at 596 n.39 (quoting Professor Arthur Miller).

[167] Under the FCRA a creditor that discloses "consumer report" information becomes a consumer reporting agency and is therefore subject to FCRA requirements. 15 U.S.C. § 1681 (2000).

[168] *Id.*

[169] *Id.* § 1681a(d)(2) (added by Pub. L. No. 104-208, 110 Stat. 308 (1996)).

[170] *Id.* § 1681s(a)(4) (1998) (containing provision that was later deleted from the act).

[171] 15 U.S.C. §§ 6801-09, 6821-27 (2000). The Act is also known as the Financial Services Modernization Act of 1999. The Act took effect in July of 2001.

[172] *See* 15 U.S.C. § 6803 (2000).

[173] *See id.* § 6802(b).

[174] *See id.* § 6802(b)(2).

brokerage firms, and insurance companies to share their respective databases with one another. However, they cannot sell customer data to third parties without providing an opt-out notice to consumers.

A parallel can be drawn between the regulation of financial and credit information and the potential regulation of charitable donor lists. As mentioned earlier, the profiling of donors consists of assessing the financial background of a given charitable donor. Information gathered to form charitable donor lists is financial in nature. Indeed, constructing a donor list containing "contributors, of $15.00 & over to heart or cancer appeals"[175] would require knowledge of a donor's financial capabilities and the amount of a donor's previous giving. Nothing could be more private and sensitive to a charitable donor than such information. The need for a federally mandated opt-out regulation in the context of charitable donors is thus apparent and necessary to the maintenance of the public's trust in charities and nonprofit entities.

5. *The USA PATRIOT Act.*

On October 26, 2001, in response to the September 11 attacks, President Bush signed the USA Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act into law.[176] The thrust of the Act and the controversy accompanying it centers on provisions that facilitate the government's surveillance of citizens' everyday activities and the collection of personal information.[177] There has been much recent scholarship on the Act addressing the constitutional, theoretical, and practical aspects of this groundbreaking legislation.[178]

---

[175] *See* W.S. Ponton, Inc., Philanthropic Donor Lists, *at* http://www.geocities.com/wsponton/pages/01philan (last visited Apr. 20, 2004).

[176] Pub. L. No. 107-56, § 1, 115 Stat. 272, 272-75 (2001) (providing title and table of contents).

[177] *See id.* § 816, 115 Stat. at 385 (creating cyber-security training for law enforcement). On the controversies surrounding the Act, see Mell, *supra* note 10, at 376 (comparing the effects of the surveillance provisions to the Orwellian Big Brother state).

[178] *See, e.g.*, Jennifer C. Evans, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933 (2002) (arguing that the PATRIOT Act represents a threat to citizens' constitutional rights); Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607 (2003) (arguing that the PATRIOT Act is not as invasive as is often portrayed); Lawrence M. Lebowitz & Ira L. Podheiser, *A Summary of The Changes in Immigration Policies and Practices After The Terrorist Attacks Of September 11, 2001: The USA PATRIOT Act and Other Measures*, 63 U. PITT. L. REV. 873 (2002) (focusing on immigration-related provisions of the PATRIOT Act and other pending legislation and administrative changes); Michael T. McCarthy, *Recent Development: USA PATRIOT Act*, 39 HARV. J. ON LEGIS. 435 (2002) (describing the PATRIOT Act as a legislative proposal and the reactions of civil liberties groups).

For recent scholarship on the infringements of civil liberties resulting from the PATRIOT Act and post-September 11th generally, see LOST LIBERTIES (Cynthia Browne, ed., 2003); DAVID COLE, ENEMY ALIENS (2003); NAT HENTOFF, THE WAR ON THE BILL OF RIGHTS AND THE GOVERNMENT RESISTANCE (2003); PHILIP B. HEYMANN, TERRORISM,

While the PATRIOT Act was geared towards combatting terrorism, several other provisions in the Act relate to the privacy rights of charitable donors and consumers alike. For instance, the Act's amendments to the Telemarketing Act[179] affected the scope of the Telemarketing Sales Rule (TSR), particularly in the context of the solicitation of charitable contributions and TSR's applicability to nonprofits.[180] First, section 1011(b)(2) of the Act adds a new section to the Telemarketing Act requiring the FTC to include in the "abusive telemarketing acts or practices" provisions of the TSR a requirement that

> any person engaged in telemarketing for the solicitation of charitable contributions, donations, or gifts of money or any other thing of value, shall promptly and clearly disclose to the person receiving the call that the purpose of the call is to solicit charitable contributions, donations, or gifts, and make such other disclosures as the Commission considers appropriate, including the name and mailing address of the charitable organization on behalf of which the solicitation is made.[181]

This new requirement is significant in that it implicitly recognizes the time costs and informational rights—if not the privacy rights—of charitable donors as a separate and distinct class of individuals.

More importantly, and perhaps more relevant to the privacy rights of charitable donors, section 1011(b)(1) of the PATRIOT Act amends the "deceptive telemarketing acts or practices" provision of the Telemarketing Act.[182] This amendment states that the FTC shall include in such rules respecting deceptive telemarketing acts and practices a definition of deceptive telemarketing acts or practices "*which shall include fraudulent charitable solicitations.*"[183] The FTC has interpreted the amendments to the Telemarketing Act effectuated by section 1011 of the PATRIOT Act together with the unchanged sections of the Telemarketing Act and has concluded that for-profit entities that solicit charitable donations must comply with the Telemarketing Sales Rule (although the TSR does not apply to not-for-profit organizations

---

FREEDOM, AND SECURITY (2003); THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN THE AGE OF TERRORISM (Richard C. Leone & Greg Anrig, Jr. eds., 2003); JEFFEREY ROSEN, THE NAKED CROWD (2003).

[179] 15 U.S.C. § 6102(a)(2) (Supp. 2003) (including fraudulent charitable solicitations in scope of regulation of deceptive telemarketing). The TSR gives the FTC and state attorneys general law enforcement tools to combat fraudulent activities carried out by telephone. Additionally, the TSR provides consumers with privacy protections and defenses against unscrupulous telemarketers. The rule prohibits misrepresentations and requires telemarketers to give consumers certain disclosures including but not limited to the seller's identity, the purpose of the call, the nature of the goods or services offered, and that no payment or purchase is necessary to win if a prize promotion is offered. Companies that violate the TSR can be subject to FTC enforcement action and fines of $10,000 per violation.

[180] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[181] *Id.* § 1011(b)(2)(D), 115 Stat. at 396.

[182] 15 U.S.C. § 6102(a)(2) (Supp. 2003).

[183] USA PATRIOT Act, Pub. L. No. 107-56, § 1011(b)(1), 115 Stat. 272, 396 (2001) (emphasis added).

themselves).[184]

The importance of these amendments with respect to the regulation and potential enhancement of the rights of charitable donors cannot be understated. The PATRIOT Act amendments bring the Telemarketing Act's jurisdiction over charitable solicitations in line with the jurisdiction of the FTC under the Federal Trade Commission Act (FTC Act) by expanding the TSR's scope to include not only the sale of goods or services, but also charitable solicitations by for-profit entities on behalf of nonprofits.[185] This indirect expansion of the FTC's jurisdiction under the FTC Act can potentially empower the agency to further regulate and safeguard the privacy interests of donors notwithstanding the fact that the FTC lacks a direct jurisdictional mandate over nonprofit entities.

B. *Comprehensive Efforts to Regulate the List Trade*

As early as 1977, consumers, recognizing that their personal information was being non-consensually gathered and sold, alerted Congress that the trade in mailing lists required comprehensive regulation.[186] The Privacy Protection Study Commission ("Privacy Commission") was directed by Congress to conduct a "study of the data banks, automatic data processing programs, and information systems . . . to determine the standards and procedures in force for the protection of personal information."[187] After conducting a comprehensive study, the Privacy Commission essentially recommended that marketers remain free to conduct their businesses with minimal interference.[188] The Privacy Commission recommended that list gatherers should inform consumers about the secondary uses they would make of information they gathered, and should provide consumers with the ability to opt-out of inclusion on lists.[189] The Privacy Commission credulously (and perhaps intentionally) believed that businesses would voluntarily adopt privacy safeguards. "A person engaged in interstate commerce who maintains a mailing list should not be required by law to remove an individual's name and address from such a list upon request of

---

[184] The FTC noted that, despite its broad mandate to regulate charitable solicitations made via telemarketing, the PATRIOT Act amendments did not expand the FTC's jurisdiction under the TSR to make direct regulation of nonprofit organizations possible. FTC, Telemarketing Sales Rule, Proposed Rulemaking, 67 Fed. Reg. 4492 (Jan 30, 2002).

[185] *Id.* For a discussion of the FTC Act, see *infra* Part VI.A.

[186] *See generally* U.S. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) (recommending that those engaged in interstate commerce who maintain a mailing list should not be required to remove an individual's name upon request except as otherwise required).

[187] David F. Linowes, *Preface to* U.S. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977), *available at* http://www.epic.org/privacy/ppsc1977report/preface.htm.

[188] *See id.*

[189] *See id.* at 1-51.

that individual," the Privacy Commission urged.[190] The Privacy Commission was swayed by the economic importance of direct mail, the reliance of nonprofit organizations and political candidates, and the impracticability of mandating a system of name removal.[191]

The Privacy Commission further recommended that consumers and *charitable donors* alike be given the option to refuse dissemination of personal information.[192] The recommendation explicitly provided that "when a private-sector organization is informed by one of its consumers, members, or *donors* that he does not want his address, or name and address, made available . . . the organization should promptly take whatever steps are necessary to assure that the name and address is not so used . . . ."[193] Thus, the need to protect consumers and donors alike was quite apparent, as both groups have similar privacy concerns. While the pioneer congressional committee on privacy was completely inaccurate in its perception of organizations that disseminate information, the Privacy Commission was foresighted about the fact that donors should be included as a protected class in any legal scheme addressing privacy concerns.

There are few reports that, in retrospect, ring as hopelessly outdated as the 1977 Privacy Committee Report. The Privacy Commission's wishful model of self-regulation has crumbled. Consumers are virtually defenseless against businesses that disseminate personal consumer information without seeking consent and with impunity.[194]

Recently, however, Congress has awakened from its decades-long neglect. Many bills that mention privacy were pending at the end of the 2000 congressional session. One of these bills that failed and is now being reintroduced, the Consumer Privacy Protection Act (Privacy Act),[195] calls for general privacy legislation.[196] The Privacy Act was introduced in the Senate on May 23, 2000, and was referred to the Senate Committee on Commerce,

---

[190] *Id.* at 147.

[191] *See id.* at 147-48.

[192] *See id.* at 151.

[193] *Id.* (emphasis added).

[194] *See* Reidenberg, *supra* note 36, at 197-98 (describing changing privacy landscape following Privacy Commission Report). There are regulations that give consumers the option to opt-out (for example, financial institutions under the GLBA are required to do so). However, most of these institutions make it difficult to opt-out and raise transaction costs for consumers who choose to opt-out. There is even a story of one consumer who mailed many opt-out letters, yet he still receives one to seven junk mail letters each day. *See* G. Bruce Knecht, *Junk-Mail Hater Seeks Profits from Sale of His Name*, WALL ST. J., Oct. 13, 1995, at B1 (describing suit brought against magazine for releasing subscriber information).

[195] Consumer Privacy Protection Act of 2000, S. 2606, 106th Cong. (2000) [hereinafter 2000 Privacy Act]; Consumer Privacy Protection Act of 2003, H.R. 1636, 108th Cong. (2003) [hereinafter 2003 Privacy Act].

[196] *See* Grant Gross, *New Privacy Laws Less Likely: Congress is Focusing on Spam, Observers Say*, PC WORLD, July 21, 2003 (describing lack of congressional citation to online consumer privacy), *available at* http://www.pcworld.com/news/article/0,aid,111659,00.asp.

Science, and Transportation, where it ultimately failed.[197] A watered down version of the 2000 bill recently has been reintroduced in the House by Representative Cliff Stearns and twenty-two co-sponsors.[198] While the scope of the Privacy Act does not reach the desired level of regulation, it does have many beneficial features.

The original Privacy Act of 2000 was to open with a startling declaration of theoretical rights: "(1) The right to privacy is a personal fundamental right worthy of protection through appropriate legislation; (2) Consumers engaging in and interacting with companies engaged in interstate commerce have an ownership interest in their personal information, as well as a right to control how that information is collected, used or transferred."[199]

The Act further would have required consumer opt-in consent (customer required to choose affirmatively) to online collection of personally identifiable information, and opt-out consent (customer permitted to decline) for non-personally identifiable information. Both the FTC and state attorneys general would have standing to sue violators, and private individuals would have standing to sue for misuse of personally identifiable information.[200] While the Act was a respectable effort to combat the problems consumers are faced with, it did not provide an avenue of recourse for charitable donors. The diluted 2003 manifestation of this Act also does not provide for privacy problems in the nonprofit context.

VI. POTENTIAL MEANS OF REDRESS FOR CHARITABLE DONORS

Apart from the possibility of a private contract-based action,[201] or of

---

[197] *See* 2000 Privacy Act, S. 2606, 106th Cong. § 2 (2000). The Committee and the FTC cooperated in hearings on Internet privacy and online profiling. *See Hearing on Online Profiling and Privacy Before the Senate Comm. On Commerce, Sci. and Trans.*, 106th Cong. (2000), *available at* http://www.commerce.Senate.gov/hearings/hearin00.html; *see also Hearing to Review the FTC's Survey of Privacy Policies Posted by Commercial Web Sites Before the Senate Comm. On Commerce, Sci. and Trans.*, 106th Cong. (2000), *available at* http://www.commerce.Senate.gov/hearings/hearin00.html.

[198] 2003 Privacy Act, H.R. 1636, 108th Cong. (2003). The bill requires companies collecting personal information to notify customers and tell them for what purpose the information is being collected. The Stearns bill also allows customers to refuse to let entities share their data in an opt-out scheme, while the original 2000 Privacy Act followed an opt-in paradigm. *See* Gross, *supra* note 196; *see also*, Press Release, Representative Cliff Stearns, Stearns Introduces Consumer Privacy Protection Act of 2003 (Apr. 4, 2003), *available at* http://www.house.gov/stearns/PressReleases/PR2003Releases/pr-030404-privacy.html.

[199] 2000 Privacy Act, S. 2606, 106th Cong. § 2(1), (2) (2000).

[200] *See id.*

[201] It is possible and perhaps desirable for donors who make gifts to nonprofits to enter into contractual agreements by which they prohibit donees from making use of knowledge of their gift in any way. For more on the ability of individuals to enter into private agreements relating to their personal privacy, see generally Jeffrey M. Lacker, *The Economics of Financial Privacy: To Opt-Out or Opt-In?*, 88/3 FED. RES. BANK OF RICHMOND ECON. Q. 1 (2002), *available at* http://www.rich.frb.org/pubs/eq/pdfs/summer2002/lacker.pdf, arguing

incidental coverage under the provisions of the statutes discussed above, charitable donors do not, currently, have any established claim for the unauthorized sharing of personal information against the nonprofit organizations to which they donate. The FTC and state attorneys general,[202] however, are governing authorities that can potentially respond to donor problems. The question that surfaces is whether these organizations have jurisdiction over nonprofits. If they do have jurisdiction, do they have authority to police this kind of activity? This Part will discuss several possible avenues for redress that donors might pursue in connection with list-related privacy rights.

A. *The FTC, the IRS, and Donor Lists*

Under 15 U.S.C. § 45(a)(2), better known as Section Five of the FTC Act, the FTC is empowered to "prevent persons, partnerships, or corporations" from using "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[203] Although this catch-all does not grant the FTC specific authority to protect privacy, over the last few years it has been construed to prohibit certain privacy invasions based on deception.[204] For example, if a company makes a promise on its website or in company literature to abide by certain practices and later breaches that promise, it may be prosecuted for committing an unfair or deceptive practice contrary to Section Five of the FTC Act.[205] Although this authority is useful, "the

---

that consumers and financial institutions are generally free to agree to alternative arrangements with respect to the dissemination of personal information.

Additionally, many givers insist on anonymity, which arguably precludes the collection of any personal information about the anonymous giver. Indeed, any such dissemination of an anonymous charitable donor's personal information would arguably undermine the donor's intent to donate anonymously.

[202] This Article will discuss the New York State Attorney General's role, specifically.

[203] 15 U.S.C. § 45 (2000). The FTC is also responsible for overseeing and enforcing the privacy provisions of the following laws: (1) The Fair Credit Reporting Act, 15 U.S.C. § 1681 (2000), which regulates the use and disclosure of "consumer reports" by consumer reporting agencies; (2) The Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108 (2000), which protects consumers from invasive and fraudulent telemarketing practices; (3) The Children's On-Line Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2000), which restricts the online collection of personal information from children under the age of thirteen; (4) The Gramm-Leach-Bliley Act, 15 U.S.C §§ 6801-6809 (2000), which provides limited "notice" and "opt-out" rights to consumers over their financial records; and (5) The Identity Theft and Assumption Deterrence Act of 1999, 18 U.S.C. § 1028 (Supp. 2003), which strengthens the criminal laws governing identity theft and charges the FTC with establishing a centralized complaint and consumer education service for victims of identity theft.

[204] *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: REPORT TO CONGRESS (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[205] *See id.* This however is certainly not a sufficient substitute for enforceable and comprehensive privacy laws.

Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practices principles . . . ."[206]

The statute, however, appears to exempt nonprofit and charitable organizations from the FTC's jurisdiction. The statute only applies to "persons, partnerships or corporations."[207] The FTC can assert jurisdiction over nonprofits if the activities of the organization resemble the activities of a business.[208] The test courts generally follow focuses attention on the effect on the consumer.[209]

In *FTC v. Saja*,[210] a fundraising organization engaged in a fraudulent fundraising practice that deliberately defrauded consumers. The FTC brought an action against the organization for violating Section Five of the FTC Act.[211] The organization defended on the grounds that the FTC has no jurisdiction over nonprofit organizations, the FTC Act limits jurisdiction to actions that are "in or affecting commerce."[212] The court was persuaded by the FTC's argument, that because the organization "solicit[s] donations throughout the country over interstate telephone lines and collect[s] the resulting pledges by mail or through United Parcel Service . . . . some of Defendant's solicitations are for the purchase of advertising in a publication . "[213] The court concluded that the "[d]efendant's activities affect interstate commerce."[214] The question of whether the sale of donor lists constitutes a commercial activity within the purview of Section Five has yet to be decided.

There are, however, cases that seek to determine the tax consequences of selling donor lists. Nonprofit organizations are generally tax-exempt.[215] The government supports this exemption to encourage public service by non-profits.[216] There is an exception to the tax-exempt status privilege: when nonprofits engage in business activities that compete with for-profit entities,

---

[206] *See id.* at 34.

[207] 15 U.S.C. § 45(a)(2) (2000); *see, e.g.*, Cmty. Blood Bank of Kansas City, Inc. v. FTC, 405 F.2d 1011 (8th Cir. 1969) (barring the FTC from asserting jurisdiction over nonprofits).

[208] *See* Tara Norgard, Note, *How Charitable is the Sherman Act?*, 83 MINN. L. REV. 1515, 1515-16 (explaining that when charities operate like businesses they are treated with the same force of law that constrains businesses).

[209] *See* FTC v. Pantron I Corp., 33 F.3d 1088, 1095 (9th Cir. 1994) (enunciating the test that focuses on whether a material representation, omission, or practice is likely to mislead consumers acting reasonably under the circumstances).

[210] No. CIV-97-0666-PHX-SMM, 1997 WL 703399, at *1 (D. Ariz. Oct. 7, 1997).

[211] *See id.*

[212] *See id.* at * 1, *2 (quoting 15 U.S.C. § 45(a)(2) (2000)).

[213] *Id.* at *2.

[214] *Id.* at *3.

[215] Section 501(c)(3) of the Federal Income Tax Code exempts an organization's income from taxation if the organization's purpose is religious, charitable, scientific, literary, educational, or public safety testing.

[216] *See generally* Committee on Exempt Organizations, *Important Developments During the Year: Exempt Organizations*, 43 TAX LAW. 1201 (1990).

that activity may be taxed as unrelated business taxable income (UBTI).[217] The purpose of UBTI is to maintain a level playing field between taxable and nonprofit organizations. Specifically excluded from UBTI are "royalties."[218] Courts have construed "royalties" to mean "a share of product or profit reserved by owner of property for permitting another to use the property."[219]

The question of whether the selling of donor lists is UBTI is important in the context of whether the FTC has jurisdiction over such claims. If the practice is considered income, the FTC arguably can exercise jurisdiction by asserting that when charities operate like businesses they are treated with the same force of law that constrains businesses. In *Disabled American Veterans v. United States*,[220] the question of whether the sale of donor lists constituted income was at issue. The Disabled American Veterans (DAV), a nonprofit organization, had an extensive mailing list of contributors that contained a wealth of information.[221] The mailing list took "considerable time, effort and expense" to maintain, and two paid employees were fully devoted to its maintenance and to rental activities.[222] The group used the mailing list for two reasons. First, the DAV solicited their own contributions.[223] Second, they allowed other nonprofit organizations to use the DAV mailing list for a fee.[224] The reason the group rented the list was to "gain additional revenue" especially "in the light of the substantial costs [DAV] incurred in the regular maintenance of its donor list."[225]

The court in *Disabled American Veterans* held that the income derived from the sale of mailing lists was taxable income—income that was subject to the UBTI statute.[226] The judge relied on the facts that the mailing list income was from a trade or a business, was regularly carried on, and was unrelated to its exempt purpose.[227] After finding the donor list income to be UBTI, the court held that the payments were not royalty income due to all the work the DAV invested in maintaining the lists.[228]

While the *Disabled American Veterans* case was a victory for the Internal Revenue Service (IRS), since then there have been only defeats.[229] No other

---

[217] *See* 26 U.S.C. § 511(a) (2000).

[218] *See* 26 U.S.C. § 512(b)(2) (2000).

[219] *See* Sierra Club v. Comm'r., 86 F.3d 1526, 1531 (9th Cir. 1996) (quoting BLACK'S LAW DICTIONARY 1330-31 (6th ed. 1979)).

[220] 650 F.2d 1178 (Ct. Cl. 1981), *aff'd*, 104 F.2d 1570 (Fed. Cir. 1983).

[221] *See id.* at 1182.

[222] *Id.*

[223] *See id.*

[224] *Id.* at 1184-85.

[225] *Id.* at 1184.

[226] *Id.* at 1185-88.

[227] *Id.*

[228] *Id* at 1189-90.

[229] *See, e.g.*, Sierra Club, Inc. v. Comm'r, 86 F.3d 1526, 1535-36 (9th Cir. 1996) (finding donor list income excluded as a royalty); Common Cause v. Comm'r, 112 T.C. 332,

case before the courts has applied the UBTI to donor list income. All such income has been found to be excludable from the UBTI as a royalty payment. The first case in which a United States Court of Appeals reviewed whether mailing list income could be excluded as royalty payments was the Ninth Circuit in *Sierra Club v. Commissioner*.[230] The Ninth Circuit held that while royalties had to be payments for the right to use intangible property, such payments could not be compensation for services.[231] After defining "royalty," the Ninth Circuit then applied it to the Sierra Club's donor list income. Since the Sierra Club did not provide any services, the court excluded the sums received from the UBTI under the royalty exclusion.[232]

Notwithstanding the formidable line of precedent against taxing income derived from list selling, the practice of selling donor lists is inconsistent with the policies of nonprofit exemption status. The policy behind granting exemption status is to allow the income to flow more directly to the charity and the public interest. The nonconsensual dissemination of donor information undermines the public trust and is therefore inconsistent with the reason why the federal government issues exempt status. How can offending the donating public by selling their often very private information without their consent be consistent with the policy of serving the public interest? The practice seems irreconcilable with the policy.

As a consequence of the donor list tax cases, it is more difficult to argue that the activity of selling mailing lists by nonprofits is commercial and therefore subject to FTC jurisdiction. Interestingly, however, in a case unrelated to donor lists, the Supreme Court may have inadvertently renewed the potential for FTC regulatory activity in the nonprofit sector. In *Camp Newfound/Owatonna, Inc. v. Town of Harrison*,[233] the Supreme Court reviewed the legitimacy of a town tax assessment against a nonprofit camp.[234] In doing so, the Court held that the status of the camps as nonprofit entities did not preclude the application of the Commerce Clause.[235] Moreover, the Court suggested that nonprofits can and do, in fact, engage in interstate commerce as providers of goods and services.[236] This important finding that nonprofits engage in commercial activity can potentially offer the FTC a way to become more active in the nonprofit sector if it chooses to do so.

Unrelated to the taxation of lists as income, the IRS in a separate context,

---

347 (1999) (holding that mailer's list rental payment is a royalty, which is excused from UBTI); Planned Parenthood Fed'n of Am., Inc. v. Comm'r, 77 T.C.M. (CCH) 2227, 2235 (1999) (stating that petitioner's income from operating a list rental business through consultants was royalty income that was excluded from taxation).

[230] *Sierra Club*, 86 F.3d at 1526.

[231] *Id.* at 1535-36.

[232] *Id.*

[233] 520 U.S. 564 (1997).

[234] *Id.*

[235] *Id.* at 572-73.

[236] *Id.* at 573.

has subtly stressed the importance of donor privacy. In 2001, the IRS reversed its position regarding public disclosure of information on Form 990, Schedule B, Schedules of Contributors to nonprofit entities.[237] IRS Schedule B requires most nonprofit entities to disclose the names, addresses, amounts, and other information relating to receipt of donations received by nonprofits.[238] Prior to Schedule B's inception in 2000, the IRS required such disclosure to appear on Line 1d on Form 990.[239] While Line 1d was not supposed to be subject to public disclosure, several inadvertent releases of donor information occurred.[240] The new Schedule B is a separate schedule that bears a prominent legend indicating that the form "is generally not open to public inspection except for section 527 organizations."[241]

The new Schedule B was said to "provide a means for the IRS to capture the non-public donor information, clearly separate it from the otherwise public Form 990 data, and withhold it from public inspection."[242] While commentators have suggested that the IRS has not done enough to seal loopholes under Schedule B,[243] the IRS's action nonetheless, is a major recognition of donor privacy interests.

B. *State Avenues of Redress*

The possibilities that currently exist for consumers and donors to challenge list trading by seeking state remedies are limited. Attorneys general have not pursued the problem of unauthorized data mining, and state courts have not permitted actions by individual donors to proceed in court.

1. *Attorneys general.*

Outside the context of the confidentiality of membership lists demanded by government offices or organization members, few state courts have considered matters of nonprofit informational privacy.[244] It might be expected, however,

---

[237] *See* Gregory L. Colvin & Marcus S. Owens, *Outline on Form 990 Donor Disclosure: Current Posture, Background, Options*, 35 EXEMPT ORG. TAX REV. 408, 408 (2002).

[238] *See id.*

[239] *See id.*

[240] *See id.*

[241] *Id.*

[242] *Id.*

[243] *See id.*

[244] The Revised Model Nonprofit Corporation Act, developed by a Committee of the American Bar Association and promulgated in a small number of states including Alabama, South Carolina, Idaho, and Wyoming, contains a provision that prohibits the commercial sale of nonprofit membership lists. Section 16.05 of the Act provides:

> Without consent of the board, a membership list or any part thereof may not be obtained or used by any person for any purpose unrelated to a member's interest as a member. Without limiting the generality of the foregoing, without the consent of the board a membership list or any part thereof may not be: (1) used to solicit money or property unless such money or

that in New York, where the State of New York's Attorney General Charities Bureau (NYAG) has been highly visible and active in charitable supervision, and where the Attorney General has subjected nonprofit organizations to criticism for failing to share lists with one another, the problem of donor lists would have been addressed. With New Yorkers donating $10 billion to various charities, this arm of the state government has been very active in policing nonprofits.[245]

The NYAG's supervisory authority over charities is derived from the common law of charitable trusts, as well as the *parens patriae* power of the state to protect the public interest in public assets donated for public purposes.[246] While the NYAG is authorized to police issues involving the public interest, there have been no instances of the NYAG addressing the issue of the nonconsensual sale of donor lists.[247]

2. *Redress in state court.*

Consumers and donors have not been effective in using state courts as an avenue of relief in the informational privacy context. Recently in *Smith v. Chase Manhattan Bank*,[248] several bank consumers sued Chase, alleging a violation of General Business Law Section 349,[249] New York's consumer

---

property will be used solely to solicit the votes of the members in an election to be held by the corporation; (2) used for any commercial purpose; or (3) sold to or purchased by any person.

REVISED MODEL NONPROFIT CORP. ACT §16.05 (1987). The statute vests authority to divulge names in the hands of the boards and not donors, without any requirement for the board to provide for any sort of opt-out by donors. Nor does the provision provide protection against the sale of non-membership information. *See also* Lodge 1380, Bhd. of Ry., Airline & S.S. Clerks v. Dennis, 625 F.2d 819 (9th Cir. 1980) (addressing the issue of whether union members should have access to union's membership lists); Sheldon v. O'Callaghan, 497 F.2d 1276 (2d Cir. 1974), *cert. denied*, 419 U.S. 1090 (1974) (requiring an international union to make a membership list available to a local union so that the local could mail its views to union members); Wirtz v. Int'l Bhd. of Teamsters, 218 F. Supp. 885 (D. Conn. 1963) (forbidding the use or disclosure of union membership lists); Local 191, Int'l Bhd. of Teamsters v. Goldberg, 303 F.2d 402 (D.C. Cir. 1962), *cert. denied*, 370 U.S. 938 (1962) (reiterating the congressional policy to limit access to union membership lists). The court discussed the limitations to accessing union membership lists:

> Congress granted only bona fide candidates for office the right to inspect a membership list of a labor organization, and such a candidate had that right only once prior to the election; that his right was only to inspect the list and not to make copies; and that the members whose names the candidate was entitled to see were only those who were subject to a collective bargaining agreement.

Id. at 406; *see generally* NORMAN I. SILBER, A CORPORATE FORM OF FREEDOM: THE EMERGENCE OF THE MODERN NONPROFIT SECTOR (2001).

[245] Telephone Interview with William Josephson, Assistant Attorney General, and Deputy Chief of the Charities Bureau (Apr. 17, 2002).

[246] *See id.*

[247] *See id.*

[248] 741 N.Y.S.2d 100 (N.Y. App. Div. 2002).

[249] N.Y. GEN. BUS. LAW § 349(a) (McKinney 1988).

protection statute that prohibits unfair and deceptive acts and practices in trade or commerce.[250] For plaintiffs to recover under this statute, they are required to prove that "the challenged act or practice was consumer oriented, that it was misleading in a material way, and that the plaintiff suffered injury as a result of the deceptive act."[251]

The complaint alleged that Chase engaged in a deceptive practice by sharing customer information with unrelated third parties in violation of its commitment to protect customer privacy and confidentiality.[252] Without providing the plaintiffs an opportunity to opt-out and without plaintiffs' consent, Chase "sold information to nonaffiliated third-party vendors, including the plaintiffs' names, addresses, telephone numbers, account or loan numbers, credit card usage, and other financial data."[253] The information provided by Chase to third-party vendors was used to create lists of consumers who might be interested in their products and services.[254] These lists were then proliferated among direct marketing and telemarketing agencies to conduct solicitations.[255] If the consumers would purchase the product or services, the third-party vendors would in turn compensate Chase with a commission of up to twenty-four percent of the sale.[256]

The appellate division affirmed the trial court's decision dismissing all causes of action for failure to state a claim.[257] The court emphasized that a "deceptive act" under Section 349, whether a representation or omission, "must be likely to mislead a reasonable consumer acting reasonably under the circumstances."[258] Furthermore, the court noted that actual injury must be proven by plaintiffs, "though not necessarily pecuniary harm."[259] The thrust of the court's dismissal of plaintiffs' claim was plaintiffs' failure to allege and/or prove any "actual injury."[260] Quoting from the complaint, the court explained that "the products and services offered to class members as a result of [Chase's]

---

[250] Almost every state has enacted similar legislation, most of which are modeled after the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2000). *See* MICHAEL M. GREENFIELD, CONSUMER TRANSACTIONS 107 (2d ed. 1991). These state laws differ from the federal act in that they provide for some form of private remedy. *See id.*

[251] *Smith*, 741 N.Y.S.2d at 102.

[252] *See id.* at 101.

[253] *Id.*; *see also*, Sovern, *supra* note 29, at 1306-20. For a more elaborate discussion of privacy as it relates to unfair trade practices and deception under state law, see generally Lawrence Friedman, *Establishing Information Privacy Violations: The New York Experience*, 31 HOFSTRA L. REV. 651 (2003).

[254] *Smith*, 741 N.Y.S.2d at 101.

[255] *Id.*

[256] *Id.*

[257] *See id.* at 102-03.

[258] *Id.* at 102.

[259] *Id.* (citing Stutman v. Chem. Bank, 95 N.Y.2d 24, 29 (N.Y. 2000); Small v. Lorillard Tobacco Co., 94 N.Y.2d 43 (N.Y. 1999); Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, 85 N.Y.2d 20 (N.Y. 1995)).

[260] *Id.*

practices of selling class members' confidential financial information included memberships in discount shoppers' clubs, emergency road service plans, dental and legal service plans, travel clubs, home and garden supply clubs, and credit card registration and magazine subscription services."[261] Noting that this was the plaintiffs' foremost claim, the court summarily decided that the only harm was that "members were merely offered products and services which they were free to decline."[262]

Instead of focusing on the fact that the plaintiffs' personal and sensitive financial information was widely disseminated absent their consent and in complete contravention to Chase's "Customer Information Principles," the *Smith* court focused on the effect of the deceptive act. The court seems to be erroneously attached to the notion of a clear and present tangible injury, a notion that undermines the social utility of state deception and unfair practices legislation. Indeed, the *Smith* court itself clearly explained that actual pecuniary loss is not a requisite for recovery under Section 349. Furthermore, the court makes no mention of the frustrated privacy expectations the consumers had every reason to rely upon.

The *Smith* decision is a recent demonstration of state courts bending over backwards to protect industry interests and disregard the privacy rights of plaintiff litigants. The court's perception of the harm as plaintiffs being "merely offered products"[263] is grossly ignorant of what the lawsuit was about in the first place—the deceptive invasion of privacy by Chase Manhattan Bank. By summarily dismissing the plaintiffs' claim, the court all but licensed Chase's behavior, irrespective of the windfall gained by the entity at the expense of the consumers' privacy. The *Smith* case represents a hurdle for both consumers and donors alike, as the case generally undermines the ability of plaintiffs to challenge such invasions of privacy in the judicial arena.

VII. BUILDING LEGAL RESPECT FOR DONOR PRIVACY

The appropriate solution to the problem of protecting donor privacy requires the adoption of three different legislative solutions. First, a federally mandated opt-out scheme applicable to donors should be devised. Second, a national "do-not-share" database applicable to nonprofit solicitation should be created. Third, the Authors recommend the creation of a statutory cause of action for damages upon a showing that a donor was defrauded as a result of a shared list.

---

[261] *Id.*
[262] *Id.*
[263] *Id.*

A. *The Mandated Federal Opt-Out Scheme*

This Article has argued that the federal and state responses to the problem of informational privacy thus far have been inadequate. While Congress and the states have recently made efforts to legislate in a manner that is favorable to consumers, there is much to be done. The FTC and state attorneys general remain essentially toothless and uninterested, respectively, with respect to the informational privacy concerns of consumers and even more so of donors. The problems consumers are faced with extend to charitable donors; however, donors have not had the benefit of laws protecting them. A clear and conspicuous opt-out standard should be employed to prevent charities from obscuring donor information.

Under a mandated opt-out system, donors would have the option to opt-out of any trading in any of their personal information. Donors who wish to maintain a high privacy level will be empowered with a choice to do so. Mandating such a system will not prove to be costly, as a simple telephone hotline or list of people who have opted out can be produced just as easily as donor-lists themselves. If the federal government will not cede to the desire of consumers for broad based reform in the privacy context, another industry-specific law giving charitable donors the right to opt-out of donor lists must be adopted.

The implementation of such a standard will not be onerous on charities, as many large foundations have already implemented privacy policies. The current privacy policy of the United Way, by way of illustration, contains the elements of a federally mandated rule:

> We obtain donor CONSENT. Our promise to our donors is that their information will not be shared or sold to other businesses or charities. We respect a donor's right to be removed from our mailing list. We never publish donor information in recognition materials without prior consent. We ensure donor information is RELEVANT. Our purpose for collection of donor data is primarily to understand: 1) who our donors are (personal or professional interests, demographics, business information, community involvement); 2) how we may improve our services to meet donor preferences and expectations, and in doing so, enhance existing relationships and improve the services we offer. We commit to keeping donor information CONFIDENTIAL and stored SAFELY. We continually review and improve methods of how donor information is shared with staff and volunteers who rely on the information to efficiently fulfill their roles. Hard copy files of specific individual information are kept under lock and key. Our computer systems and web site are both secure, ensuring donor information is protected from public view. We are APPROACHABLE and ACCOUNTABLE.[264]

Many organizations have similar privacy policies, including some that give

---

[264] *See* United Way's website *at* http://www.securewebexchange.com/calgaryunitedway.org/donation/Our%20Commitment%20to%20Donor%20Privacy%20_website%20version_.pdf (last visited Apr. 26, 2004).

donors the opportunity to opt-out from any sharing of information.[265] The need for these policies to be mandated with the force of law rather than be voluntary is premised on the analysis above: neither the for-profit nor the nonprofit marketplace can protect privacy adequately if some organizations offer personal information protection but others do not.

Charitable giving, moreover, is based on public trust and confidence. Any undermining of this trust will ultimately impair the nonprofit organizations and the causes to which they provide much needed aid. The problem of donor privacy is a genuine concern that most donors consider first and foremost. When adults were asked if they feel it is "okay or NOT okay for a charity to share personal information like your name or address with others in order to raise additional money for programs?" a resounding eighty-five percent of adults chose "not okay."[266] Even when donors were reminded that "selling donor lists can be an important source of income for a charity, 82% of adults say charities should *always* give donors the option of taking their name off of any list that might be shared with an outside organization."[267] In the area of online giving, there already has been a giving deterrent that is attributed to the lack of privacy protection. The reasons for most donors' hesitancy in making online donations are privacy concerns and the reluctance to make financial transactions online.[268]

These empirically based concerns about donor consensus would be expressly addressed by giving charitable donors their privacy back via a mandatory opt-out scheme. A clear, conspicuous, and frequently recurring opportunity to opt-out should be the bare minimum for charitable organizations.[269] An appropriate safe-harbor, easy to understand "uniform opt-out form," together with recommended procedures for offering an opt-out alternative (or alternatives), could be implemented universally by all charitable organizations.[270] Such an opt-out should also explain the consequences of

---

[265] *See, e.g.*, American Heart Association, Policy on Collection and Use of Personal Information, *at* http://www.americanheart.org/presenter.jhtml?identifier=11404 (last visited, Apr. 20, 2004).

[266] PRINCETON SURVEY RESEARCH ASSOCS., BBB WISE GIVING ALLIANCE DONOR EXPECTATIONS SURVEY: FINAL REPORT 7 (2001), *available at* http://www.give.org/news/Donor%20Expectations%20Survey.pdf. The national survey was given to over 2000 survey respondents and was conducted in the spring of 2001.

[267] *Id* at 7.

[268] *Id.* Along the same lines, fewer than one in ten people report having ever made a charitable contribution of ten dollars or more on the Internet. *Id.* at 6.

[269] The effectiveness and application of alternative models (e.g., mandated opt-in, economic disincentives—the Ayres/Funk Model and obtaining directorial consent) will be discussed immediately *infra* text accompanying notes 285-307.

[270] Indeed, a study conducted by Jeff Sovern revealed that most consumers do opt in when given the choice. This empirical study undermines the theory that if a mandated opt-out initiative existed, no donors would allow their personal information to be disseminated. *See* Sovern, *supra* note 35. This argument however, presupposes that the characteristics of donors and consumers are comparable.

declining to opt-out in reasonably comprehensible language.

The discussion above has not only mentioned concerns about the sharing of personal information to third parties; it has also included information regarding the sharing of personal information within organizations and the subsidiaries and partners of organizations. To be effective, any comprehensive approach to donor privacy protection should include opportunities for donors to take themselves off or opt-out of intra-organizational list-shares as well as inter-organizational ones.

B. *The "Do-Not-Share" Database*

The popularity and success of the "do-not-call" database in limiting commercial telemarketing solicitations[271] suggests that this experiment could be broadened to protect personal information as well. A registry of persons who do not want any information they provide to be sold, traded, or exchanged would be a positive step in the direction of privacy protection. Just as the do-not-call registry encountered fierce opposition in the form of court challenges from affected marketers, it is likely that a do-not-share database would be subjected to similar constitutional challenges involving the impairment of an organization's right to free speech.[272] In light of the Tenth Circuit's upholding of the do-not-call scheme in *Mainstream Marketing Services, Inc. v. FTC*,[273] the creation and existence of such a database appears to survive constitutional scrutiny because the purpose of the database facilitates the contractual understandings between the parties and does not restrict free speech rights of sellers or gift recipients.

In *Mainstream*, the Tenth Circuit held that the exclusion of nonprofits from the do-not-call registry did not invalidate the entire scheme. In doing so, the

---

[271] *See, e.g.*, Associated Press, *Do-Not-Call List Continues to Expand*, WALL ST. J., Aug., 7, 2003, at B6; *Business: Don't Call Me*, N.Y. TIMES, July 13, 2003, § 4, at 2. ("Americans have submitted at least 23 million phone numbers for the federal do-not-call registry. This far exceeds the government's initial expectations. It is as if one-fifth of all American households suddenly put 'no soliciting' signs on their front doors."); Matt Richtel, *Feelings Mixed, Millions Enroll To Block Calls*, N.Y. TIMES, July 10, 2003, at A1.

While the "do-not-call" registry applies to for-profit telemarketers who conduct interstate solicitations of charitable contributions, the personal information of charitable donors is in no way protected under this model. *See* FTC Release, FTC Announces Final Amendments to Telemarketing Sales Rule, Including National "Do Not Call" Registry (Dec. 18, 2002), *available at* http://www.ftc.gov/opa/2002/12/donotcall.htm.

[272] The "do-not-call" scheme was challenged on First Amendment grounds. *See* DoNotCall.com, *ATA Launches Legal Challenge Against New Rules* (2003), *at* http://www.donotcall.com/lawsuit.asp. As stated, no First Amendment message would be suppressed by the creation of a "do-not share" database in the donor list context. *See* Matt Richtel, *Technology Briefing Telecommunications: 'Do Not Call' List Challenged*, N.Y. TIMES, July 29, 2003, at C4.

[273] 358 F.3d 1228 (10th Cir. 2004) (reversing a lower court ruling invalidating the do-not-call scheme on First Amendment grounds).

court overturned a federal court's decision that found the registry unconstitutional because it barred solicitations from companies while allowing calls from charities and politicians. The Tenth Circuit's decision does not imply the inability of the FTC to establish a nonprofit database. The court's finding that the registry was a valid restraint on commercial speech does not speak to the constitutionality and validity of a similar nonprofit database. Indeed, in a footnote, the court noted that the constitutionality of a list applicable to nonprofits and politicians is a separate constitutional question.[274]

The purpose of a do-not-share database would be to place all those organizations that agree to receive donations from those who have registered with the database on notice that all gifts from the registered donors are conditioned on an understanding of strict personal information privacy. As such, a donor would be effectively placing a condition on his donation. As a matter of contract law a donor has a right to make a gift based on a condition of anonymity, a fortiori, it is contractually permissible to condition gift-giving on withholding the personal information of the donor.

The "do-not-call" model can be easily applied to the nonprofit privacy context. Just as consumers are able to make requests to stop unwanted telemarketing calls via the Internet or on a toll-free hotline,[275] charitable donors using similar mediums can opt to withhold their consent from nonprofits that trade in personal information. Under this model, much like the "do-not-call" model, nonprofits would be required to download the registry database and remove all registered donors from their lists (thereby precluding the selling, renting, or bartering of the donor's personal information) at least once every ninety days.[276] A nonprofit that fails to comply with a donor's request can be subject to fines.[277]

In essence, a "do-not-share" database would be a government sponsored opt-out opportunity, as donors, to receive protection, would be required to affirmatively sign onto the database to protect the nonconsensual dissemination of their names, contact information, the amount and causes to which they donate, and other information. The appeal of such a database as a solution to the donor privacy problem lies in the relatively simple way of creating such a database and the low transaction costs for donors, the government, and nonprofits in maintaining the database. A do-not-share model of this type

---

[274] *See id.* at 1233 n.2.

[275] With respect to the "do-not-call" list currently in place, consumers can register online at http://www.donotcall.gov or via a toll-free hotline by calling 1-888-382-1222.

[276] *See* FED. TRADE COMM'N, CALLING ALL TELEMARKETERS: AMENDMENT TO THE FTC'S TELEMARKETING SALES RULE (2003), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/calling.pdf.

[277] Telemarketers who violate the amendments to the Telemarketing Sales Rule or an individual's do-not-call request could be subject to fines of up to $11,000. *See* Fed. Trade Comm'n, Q&A for Telemarketers and Sellers About the Do Not Call Provisions of the FTC's Telemarketing Sales Rule, *at* http://www.ftc.gov/bcp/conline/pubs/alerts/dncbizalrt.htm (last visited Apr. 20, 2004).

would preserve the privacy expectations of charitable donors who subscribe.[278]

C. *The Creation of a Statutory Cause of Action*

Whether on a state-by-state basis or through a single federal statute, a right of action against a person or entity who shares information notwithstanding an opt-out should be specified legislatively. Just as Dean Prosser's common law privacy tort paradigm protects against the invasion of privacy,[279] a similar private right of action should be available to charitable donors whose personal information has been nonconsensually misappropriated for a commercial purpose.[280]

The tort of misappropriation involves the use of an individual's name or likeness for a commercial profit.[281] In essence, when a charity is disseminating a donor's personal and confidential information for a profit, they are misappropriating what the donor holds most private. The misappropriation privacy tort, however, has traditionally applied to cases involving public figures "who do not seek privacy but on the contrary seek out opportunities for public disclosure."[282] A claim based on informational privacy will not succeed on a common law misappropriation tort theory. Therefore, it behooves state legislatures and Congress to plug this widening gap in the law by enacting provisions containing an express private right of action—something they have thus far neglected to do.[283]

Given the scarce resources of state attorneys general to enforce, the principal incentives to share information notwithstanding the express wishes of donors, and the overarching risk that disregarding donor privacy rights could undermine confidence in the nonprofit sector, a private right of action should

---

[278] Facilitation by the government of contract terms designed to prevent one-sidedness in consumer transactions has not been problematic in other contexts. For instance, the FTC's Holder in Due Course Rule, 16 C.F.R. § 433.1(c), 443.1(e) (2004), generally prohibits sellers and creditors from using contractual language denying consumers protections provided under state contract and other commercial laws.

[279] *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383, 389-407 (1960).

[280] The four torts deriving from the common law "right to be let alone" are "intrusion upon seclusion," "public disclosure of private facts," "false light," and "misappropriation." This Part will primarily focus on misappropriation. *Id.* at 389. These torts have been largely codified by several jurisdictions. *See, e.g.*, CAL. CIV. CODE § 3344 (West 1997); FLA. STAT. ANN. § 540.08 (West 2002); IND. CODE §§ 4-1-6-1 to -9 (2002); MASS. ANN. LAWS ch. 214, § 3A (Law. Co-op. 1999); N.Y. CIV. RIGHTS LAW §§ 50-52 (Consol. 1992 & Supp. 2004); R.I. GEN. LAWS §§ 9-1-28 to -28.1 (1997); RESTATEMENT (SECOND) OF TORTS § 652A app. reporter's note (1989 & Supp. 1990) (noting the states that have adopted privacy torts in one form or another).

[281] *See* Prosser, *supra* note 279, at 402-07.

[282] DAN DOBBS, THE LAW OF TORTS 1198 (2000) (noting that misappropriation tort generally safeguards celebrity status).

[283] All the government responses to the privacy problem discussed in Part V fail to provide constituents with a private right of action. Rather, Congress has relegated the enforcement of these privacy rights to the FTC.

be available for charitable donors.[284] A distinct parallel can certainly be drawn between information containing the amount and to what causes an individual donates and the "sensitive" classification in the Online Privacy Protection Act. Charitable donors are no less deserving of a forum in which they can exercise their rights to keep their confidential information private. A legislatively specified statutory cause of action would accommodate these important concerns.

D. *The Application of Alternative Models*

There have been several other models attempting to remedy the problem of privacy in the consumer context. First, Ian Ayres and Matthew Funk have recently proposed that a "market for personal information" be created that will produce economic disincentives in the form of direct compensation to consumers from the entities that trade in the personal data.[285] Second, the notion that individuals be given the opportunity to opt in before their information is sold or traded will be assessed in the nonprofit context. An opt-in like regime is currently in place in Canada under the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). This Part will attempt to apply these alternative models to the nonprofit context and reveal their shortcomings and deficiencies regarding the distinct nonprofit privacy arena.

1. *The Ayres-Funk market approach model.*

Ian Ayres and Matthew Funk have recently attempted to formulate a market solution to the negative externalities stemming from telemarketing solicitation, junk mail, and spam email.[286] The Ayres-Funk model proposes to allow individual consumers to choose the price per minute they would like to receive as compensation for listening to telemarketing calls.[287] Such a "name your own price" mechanism would be implemented by crediting consumers' phone bills for any commercial solicitations they agree to hear.[288] This model

---

[284] *Contra* Ronald L. Plesser & Stuart P. Ingis, *Limiting Private Rights of Action in Privacy Legislation*, *at* http://www.cdt.org/privacy/ccp/privaterightofaction1.shtml (last visited Apr. 20, 2004) (arguing that "[p]rivate causes of action in privacy statutes offer incentives for class action lawyers, and result in the spending of significant amounts of money to defend lawsuits raising technical claims.").

[285] Ayres & Funk, *supra* note 105 and accompanying text.

[286] *See id.*

[287] *Id.* at 101.

[288] *Id.* at 101-08. Interestingly, Ayres and Funk also posit that such a scheme would be beneficial to the telemarketers as well. Once consumers are voluntarily opting to receive telemarketing calls (in return for tailored compensation), it becomes possible to deregulate the telemarketers—lifting current restrictions on the time (no night time calls) and manner (no recorded calls). For example, if the prohibition against tape-recorded messages were

imposes economic disincentives on telemarketers and direct marketers, and further encourages telemarketers to screen contacts more effectively to locate consumers who are more likely to be interested in their solicitation.

The market approach model effectuates consumer compensation for the calls they agree to receive and those calls would presumably be more narrowly tailored to the consumer's personal interests.[289] The consumer generally establishes the price to be paid by the telemarketers, though the approach does contemplate a possibility of the telemarketers setting the price.[290] Each individual household establishes its compensation price and the telemarketers discretionarily call the households they wish to solicit.[291]

Applying such an economic incentive-based model to the nonprofit context presents difficulty for Ayres and Funk. Conceptually, they find it to be counterintuitive and inconsistent with the purpose of soliciting for charitable contributions to impose a compensatory cost on telemarketers for doing so.[292] Charitable solicitations are to some degree positive externalities—there may be positive third-party externalities to the solicitations that trump the donor's interest in being left alone. Because charitable solicitation produces a sufficient third-party benefit—namely to those in need of the charities services or funds—and after dabbling with a theory of government subsidized compensation to donors, Ayres and Funk ultimately suggest that charitable solicitation be exempt from the duty to compensate.[293]

Although the proposal is new and the case unproven, there is a stronger argument than Ayres and Funk acknowledge for extending their proposal to nonprofits as well as for-profits. First, it is much more than the donor's wish to be left alone that is at stake on the detrimental side of the equation. Second, there are distinctions to be drawn in the types of nonprofit solicitations that potential donors receive which might warrant extending their proposal to some nonprofits, if not all of them. Third, there is little evidence to indicate that the net effect of the proposal would be to diminish the general level of charitable giving. Finally, there are precedents for applying the Ayres-Funk proposal to nonprofits as well as for-profits.

The extent to which the externalities are positive in the aggregate depends upon the parties to whom lists are sold for the purpose of solicitations. Surely

---

repealed, we could imagine local grocery stores or movie theaters using the telephone to provide consumers with useful information about specials. And faced with increasing caller resistance, we imagine that survey groups, such as the Gallup Poll, might welcome the opportunity to compensate survey respondents so that they might be able to produce more representative samples. *See id.* at 78..

[289] *See id.* The telemarketer is likely to set up an automated program refusing to call consumers who have posted prices that exceed some maximum amount.

[290] *See id.* at 113.

[291] *See id.*

[292] *See id.* at 118.

[293] *See id.* at 119 ("[C]haritable contributions further more general public interests or that political communications help secure better government for all.").

there is no positive externality in deterring telemarketing fraud and identity theft, pervasive problems that are as significant in nonprofit as for-profit solicitations.[294] Recent indications are that there is a direct relationship between the sharing of donor lists and the likelihood of both fraud and theft.[295] The costs associated with identity theft and fraud resulting from nonprofit charitable solicitations are great[296] and should be added to any calculus attached to the donor's need to be left alone.

Even if the positive benefit to third-party charities (considering only those the potential donor did not know about) is larger than the harm done to donors in the aggregate, furthermore, there are distributional effects on particular classes of potential donors to be taken into account, particularly among the elderly, the very young, and the poor. Just as many consumer protection statutes are directed at discrete classes of especially vulnerable consumers, so

---

[294] On the frequency of identity theft due to tenuous personal information standards, see generally, Nicole M. Buba, Note, *Waging War Against Identity Theft: Should the United States Borrow from the European Union's Battalion?*, 23 SUFFOLK TRANSNAT'L L. REV. 633 (2000); Brandon McKelvey, Comment, *Financial Institutions Duty of Confidentiality To Keep Customers' Personal Information Secure from the Threat of Identity Theft*, 34 U.C. DAVIS L. REV. 1077 (2001). Fraudulent charitable solicitation has always been a concern. *See* Fed. Trade Comm'n, Charitable Donations: Give or Take?, *at* http://www.ftc.gov/bcp/conline/pubs/tmarkg/charity.htm (last visited Apr. 20, 2004).

[295] Indeed the FTC has cited to several reasons as to how the crime of identity theft is perpetrated, one being the "use [of] personal information you share on the Internet" and another involving the purchasing and selling of personal information. Fed. Trade Comm'n, Id Theft: When Bad Things Happen To Your Good Name, at www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm (last visited Apr. 20, 2004). Additionally, the FTC has launched a campaign, advising people to manage to the best of their ability the availability of their personal information. "By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft." *Id.*

[296] The following facts signify the prevalence and costs of identity theft:

- In 1992 TransUnion received only about 35,000 calls about identity theft, from victims and those concerned about potential crime. In 2001 they received more than a million calls.
- It is estimated that 700,000 to 1.1 million people became victims of this crime in 2001. That number is based on various reports including those from members of law enforcement.
- The Secret Service estimates that in 1997 consumers lost more than $745 million due to identity theft.
- A Florida Grand Jury estimated that the average identity theft crime costs the business community about $17,000 per victim. (report found under Speeches). If we use the number 700,000 victims, that means a loss of $11.9 billion in 2001.
- This number does not include victim costs including legal assistance, judicial and law enforcement time in investigating and trying cases.
- A GAO study on identity theft (GAO-02-363, issued March 2002) discussed costs to federal agencies—The executive office for U.S. Attorneys estimated cost of prosecuting a white-collar crime case was $11,443. The Secret Service estimates the average cost per financial crime investigation is $15,000. The FBI estimates the average cost per financial crime investigation is $20,000.
- On average, victims spend 175+ hours and $1,000 in out-of-pocket expenses to clear their names. (Privacy Rights Clearinghouse and FTC).

Identity Theft Resource Center, Facts and Statistics, *at* http://www.idtheftcenter.org/html/facts_and_statistics.htm (last visited Apr. 20, 2004).

the metering proposal could in principle be applied to some or all of these groups.

There is also a possibility, concededly speculative, that any decrease in nonprofit revenues resulting from the Ayres-Funk proposal would not occur in proportion to increased costs resulting from metering nonprofit solicitations. The present-day permissibility of intercompetitive solicitation by charities may well impose a high "intra-brand" fundraising expense effect. Much of the tobacco industry claims that the high advertising budgets of the various brands shift consumption patterns from one brand of cigarette to another but do not have an impact on overall consumption levels,[297] so it may be true that solicitations by charities affect the particular choice, but not the general level, of charitable spending. Viewed in this light, any diminished revenue to nonprofits could be offset by the possibility of a shift in the general proportion of nonprofit resources that are devoted from marketing and solicitation to activities more directly related to charitable missions.

Finally, there are precedents for imposing metered costs on the nonprofit list trade. Expensive postage costs are currently attached to charitable solicitations that surely fall into the category of fundraising disincentives. The Ayres-Funk proposal essentially provides donors with an option to have "Postage Paid By Addressee," applicable not just to postage, but to telephonic, email and other forms of solicitation. In the case of postage, however, the costs being defrayed are directly related to the labor involved in conveying the solicitation; and in the proposal the costs defrayed are the estimated costs to donors of processing the messages they receive. To the extent that donors could choose to impose no cost whatsoever upon the sender, it is not likely that the proposal, if applied equally to for-profits and nonprofits alike, would face an insurmountable constitutional impediment.

Compensating a donor for consent to trade in the donor's personal information would not necessarily be counterintuitive. And yet such a proposal may be more extreme and administratively difficult than would be necessary to achieve a substantially optimal level of donor privacy. One possibility would be to amend the Ayres-Funk suggestion by imposing monetary disincentives on nonprofits that trade in donor lists by way of taxing the list trade rather than imposing bureaucratic and other costs on individual donors.

2. *The mandatory opt-in model.*

A mandatory opt-in model would require affirmative steps by charitable donors to allow the collection and/or use of information. If the charitable donor does not affirmatively act to allow the nonprofit to use his or her personal information, the entity is forbidden from doing so. Professor Jeffrey Sovern,

---

[297] *See* ASH.org, Factsheet no.19: Tobacco Advertising and Promotion (2004), *at* http://www.ash.org.uk/html/factsheets/html/fact19.html.

along with others, has proposed such a solution in the for-profit context as the best way to honor the consumer interest.[298] A recent Federal Communications Commission (FCC) ruling illustrates how an opt-in would function in practice. After interpreting the Telecommunications Act of 1996, the FCC issued a ruling that phone companies seeking to utilize calling patterns for marketing and other similar purposes must first obtain the consumer's express consent.[299] The telephone companies were required to seek the consent of consumers and in many cases attempted to do so by sending mailings to subscribers.[300]

Similarly, under Canadian law, effective January 1, 2001, if a Canadian charity seeks to use the personal information of charitable donors for a purpose that deviates from the one for which it was originally collected, the charity would be required to obtain consent from the donors beforehand.[301] The Personal Information Protection and Electronic Documents Act (PIPEDA)[302] establishes rules for how private sector organizations—including nonprofits—may collect, use or disclose personal information in the course of commercial activities.[303] The Act defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of commercial character, including the selling, bartering or leasing of *donor, membership or other fundraising lists*."[304]

These express provisions of the PIPEDA effectively function as an opt-in protection for charitable donors. This protection raises the question of whether a mandatory opt-in model is desirable and/or economically feasible given the delicate competing interests inherent in the nonprofit arena.

---

[298] *See* Sovern, *supra* note 35, at 1034; Jeff Sovern, *Helping Consumers Protect Their Personal Information*, 12 ADVANCING THE CONSUMER INTEREST 23 (2000).

[299] *See* Telecommunications Carriers' Use of Customer Propriety Network Information and Other Customer Information, 63 Fed. Reg. 20,326 (Apr. 24, 1998) (to be codified at 47 C.F.R. pt 22, 64); *see also* U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

[300] For a discussion on the effectiveness of opt-in privacy measures in the consumer privacy context, see generally Sovern, *supra* note 35.

[301] *See* Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000 ch. 5 (Can.). Part 1 of the Act (Personal Information Protection) establishes rules governing the collection, use, and disclosure of personal information and Part 2 (Electronic Documents) addresses the use of electronic alternatives to paper. This Act took effect on January 1, 2001. The Act applies to the disclosure of personal information across provincial and territorial boundaries.

[302] The Act is available in its entirety on the Canadian Privacy Commissioner's website, *available at* http://www.privcom.gc.ca/legislation/02_06_01_e.asp (last visited Apr. 20, 2004).

[303] For a comprehensive discussion of PIPEDA's personal information provisions, see generally Erika King & John H. Fuson, *An Overview of Canadian Privacy Law for Pharmaceutical and Device Manufacturers Operating in Canada*, 57 FOOD DRUG L.J. 205 (2002).

[304] *See* PIPEDA, S.C. 2000 ch. 5, § 2(1) (emphasis added). For a discussion of the scope of PIPEDA's coverage, see Juliana M. Spaeth, et al., *Privacy, Eh!: The Impact of Canada's Personal Information Protection and Electronic Documents Act on Transnational Business*, 4 VAND. J. ENT. L. & PRAC. 28, 33 (2002).

While protecting donor privacy is of vital importance, nonprofits have a significant competing public interest in effectively fundraising for their underlying charitable causes—an interest not present in the consumer privacy context. Fundraisers generally spend between twenty and forty cents for each dollar of donations they raise.[305] These costs result from transaction and origination costs, namely the labor, printing, postage, solicitation, administration, and other miscellaneous expenses associated with fundraising campaigns. A recent study suggested that an opt-in data restriction in the nonprofit arena would increase administrative costs for charities by thirty percent, thereby causing the charities to expend approximately fifty-three cents to raise each dollar of donations.[306] The study estimates that should an opt-in model become law, "approximately $16.5 billion currently allocated to charitable programs will be spent on additional marketing costs."[307]

As discussed earlier, nonprofit fundraising is dependant on hundreds of millions of dollars generated by the selling, renting, and bartering of donor lists.[308] Donor lists are arguably the best source of data for marketing and fundraising purposes. An opt-in model is certainly a more aggressive (and possibly more effective) way of addressing the consumer privacy problem, however, in the consumer realm the public's interest in the funds of nonprofit charities is not present. The unintended cost consequences of an opt-in model could potentially undermine nonprofit fundraising, which in effect, could prove to be harmful to those dependent on charitable funds. There are also constitutional impediments to be considered in proposing a legislated mandatory opt-in approach. Since this additional delicate dynamic is present in the nonprofit context, the Authors believe mandatory opt-in data restriction would be inconsistent with the public's interest in maximizing funds for charitable purposes. The mandatory opt-out proposed by the Authors would afford donors with the privacy protection they deserve and appropriately balance the fundraising goals of charitable organizations for the public interest.

VIII. CONCLUSION

Recent surveys suggest that public confidence in nonprofits has declined considerably.[309] The public's confidence "affects almost everything that

---

[305] *See* MICHAEL A. TURNER & LAWRENCE G. BUC, THE IMPACT OF DATA RESTRICTIONS ON FUNDRAISING FOR CHARITABLE & NONPROFIT INSTITUTIONS 4 (2002), *available at* http://www.infopolicy.org/documents/charity.doc.

[306] *See id.* at 3-4. The study was based on interviews with nonprofit fundraising experts from diverse sectors, fundraising data, and publicly available nonprofit data.

[307] *Id.* at 5.

[308] *See* Meeks, *supra* note 38 and accompanying text.

[309] *See* The Brookings Institution, *As End of Year Giving Season Kicks Off, Public Confidence in Charitable Organizations Remains Shaken* (2002), *at* http://www.brookings.edu/comm/news/20021210nonprofits.htm. Indeed more than half of people surveyed had "fair" or "not too much" confidence in charitable organizations. A little over ten percent of

matters to the future of the nonprofit sector, especially the public's willingness to contribute money and volunteer time. Even a small decline in confidence should raise alarms across the sector."[310] A survey conducted in 2003 by the Federation of Nonprofits revealed that nine out of ten donors want the chance to take their names off donor lists before they are exchanged. Moreover, a donor bill of rights drafted and approved by several large nonprofit organizations in recent years[311] unequivocally recommends that donors should have "the opportunity for their names to be deleted from mailing lists that an organization may intend to share."[312] In the words of Charles Fried, "[privacy] is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust," because these relations necessitate "a context of privacy for their existence."[313] The time has come to empower charitable donors with a choice: a choice that is responsible and considerate to their personal privacy, and a choice that enhances and protects the trust in the nonprofit sector. Adopting the solutions recommended in this Article would move the law toward accomplishing these essential objectives.

---

survey participants had "no confidence at all" in charities.

[310] *Id.* (quoting Paul C. Light, Director of The Brookings Center for Public Service).

[311] Some of these foundations include: The American Association of Fund-Raising Counsel, Association for Healthcare Philanthropy, Council for Advancement and Support of Education, and the Association of Fundraising Professionals.

[312] Council for Advancement and Support of Education, Donor Bill of Rights, *at* http://www.case.org/Content/AboutCASE/Display.cfm?CONTENTITEMID=2569 (last visited Apr. 20, 2004).

[313] Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968); *see also* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 451 (1980) (stating that privacy promotes individual liberty, autonomy, and personal enrichment).