No. 295 **January 22, 1998**

Policy Analysis

PRIVACY AS CENSORSHIP
A Skeptical View of Proposals to Regulate Privacy in the Private Sector

by Solveig Singleton

Solveig Singleton (formerly Solveig Bernstein) is director of information studies at the Cato Institute.

Executive Summary

Some privacy advocates urge the adoption of a new legal regime for the transfer of information about consumers among private-sector databases. This "mandatory opt-in" regime would require private businesses to ask for a consumer's permission before trading information about that consumer, such as his buying habits or hobbies, to third parties. This would, in effect, create new privacy rights.

These new rights would conflict with our tradition of free speech. From light conversation, to journalism, to consumer credit reporting, we rely on being able to freely communicate details of one another's lives. Proposals to forbid businesses to communicate with one another about real events fly in the face of that tradition.

New restrictions on speech about consumers could disproportionately hurt small businesses, new businesses, and nonprofits. Older, larger companies have less need for lists of potential customers, as they have already established a customer base.

We have no good reason to create new privacy rights. Most private-sector firms that collect information about consumers do so only in order to sell more merchandise. That hardly constitutes a sinister motive. There is little reason to fear the growth of private-sector databases.

What we should fear is the growth of government databases. Governments seek not merely to sell merchandise but to exercise police and defense functions. Because governments claim these unique and dangerous powers, we restrict governments' access to information in order to prevent abuses. Privacy advocates miss the target when they focus on the

growth of private-sector databases.

New "Phone Book" Raising Serious Privacy Issues

> Palo Alto, CA--Alarmed by the "ever-shrinking security and rights of individuals in the information age," the Palo Alto-based group Citizens For Privacy is calling for strict controls to be placed on "phone books"--printed directories of all the telephone numbers in a specified area. "With this new piece of technology," CFP head Nadine Geary said, "anyone could know your phone number in literally seconds." Exacerbating the situation, Geary said, is the fact that, in many cases, the subject's address is also printed right next to the number. "If this device is allowed to be distributed," Geary said, "literally anyone would be able to track you down at any time. It's frightening."
>
> The Onion[1]

Should private companies be permitted to keep information about customers' buying habits and identities and share that information with other businesses? Or do we own such information about ourselves, giving us the right to control its transfer from one business to another?

This paper explores the tangled moral and economic issues surrounding the collection and transfer of information about consumers by businesses using the Internet and other networks. It concludes that we have little to fear from private collection and transfer of consumer information; our attention should shift to threats from government databases.

One survey reports that the number of people "somewhat concerned" about threats to their privacy (government and private) grew from 64 percent in 1978 to 82 percent in 1995.[2] Internet users' concerns about what might happen to data collected from them online may be holding back electronic commerce.[3] But some "feel that the public's concern for privacy is like the River Platte, a mile wide but only an inch deep."[4]

Public concern about data collection may have shifted from government databases to private databases.[5] Journalists, who usually fail to distinguish between the two types of databases, bear at least some responsibility for this. One observer comments that "the public's concerns are fueled by a steady supply of articles and television programs about the dire

implications of data-driven marketing. 'The right to privacy has all but disappeared,' says a typical account in USA Today, 'sacrificed on the altar of customer service and corporate profits.'"[6]

But this paper will argue that there is no justification for regulating the collection and use of data by the private sector. Regulations intended to protect privacy by outlawing or restricting the transfer of consumer information would violate rights of free speech. The formal mechanisms that businesses have developed to transfer information about consumers, borrowers, and other businesses serve valuable economic and social purposes formerly served by person-to-person informal information networks.

Furthermore, the creation of new privacy rights such as mandatory opt-in and restrictions on the sale of lists of customer information would have pernicious economic effects. Well-established, older companies that have collected consumer information for years would have an advantage over new companies, which, to get started, must rely on lists that sort consumers by their interests and preferences. Some more extreme regulatory solutions that would bar the use of existing customer lists are no better; they would make marketing as a general matter much more burdensome, which again would work to the advantage of established companies.

Although some laws intended to protect privacy would clearly be harmful, not all concerns about privacy lack merit. Government-run databases present a terrible danger to civil liberties.[7] Consumers have long-held expectations, backed by contract and custom, that information given to professionals such as doctors and lawyers will be kept confidential. This paper, however, focuses on private rather than government databases, and on ordinary transactions (say, the purchase of shoes or garden supplies) rather than contracts for professional services.

The Dubious Origins of Privacy

Scholars in the area of medical ethics have long explored the idea of privacy as one's right to give consent before information about oneself is relayed to third parties, a context where the idea clearly makes sense.[8] Increasingly, though, privacy advocates assert that people have a general right to control the use of information about themselves, implying that

anyone wishing to transfer or collect almost any kind of information should first get the permission of the person whom the information concerns.[9] This analysis focuses on that specific concept of "privacy," though privacy can be (and probably should be) otherwise defined.[10]

Outside the medical context, the idea of privacy as applying to personal information has very dubious origins. From ancient Athens to the late 19th century, the enforcement of laws protecting private property naturally provided protection for privacy. Generally, privacy was not considered a right independent of property rights, as long as those collecting the data were in the private sector.[11] There were, however, limitations on the power of governments to collect information, such as the Fourth Amendment.[12]

Following the publication of an article by Louis D. Brandeis (later Justice Brandeis) and Samuel D. Warren in 1890, statutes and the common law increasingly began to recognize rights to privacy independent of ordinary physical property rights. The authors' inspiration was their concern that "the press is overstepping in every direction the obvious bounds of propriety and of decency"[13]--a concern echoed today in the outcry against the "paparazzi." Warren, in particular, was irritated to find details of his home life described in the society pages of the Boston press.[14] Brandeis and Warren argued in favor of the creation of a new kind of property right in personal information. Among other unfortunate omissions,[15] however, they failed to consider whether creating new rights to restrict the press would violate principles of free speech.

The Brandeis and Warren article gave birth to a hodge-podge of privacy torts.[16] Some states enacted privacy statutes of limited scope.[17] Even in later years, courts and commentators only occasionally recognized the conflict between privacy and free speech.[18] Fortunately, though, the new torts and statutes were narrowly defined.[19] The general rule remains that human beings enjoy the freedom to converse and trade information about one another in most contexts, as they have always done.

Recent Developments in Privacy

Fear of new computer network technology (especially the Internet) has combined with the development of databases that use this technology to provide a powerful emotional impetus for the creation of new privacy rights that potentially affect all

media.

Privacy groups have made the public aware that web sites can surreptitiously collect and keep information such as a visitor's e-mail address.[20] Yahoo offers a service that identifies the name associated with a given phone number, like a reverse phone directory.[21] Internet commerce raises the growing possibility that businesses will be able to track an individual's purchasing habits and credit information without that individual's knowledge.[22]

In response to concerns about the use and abuse of personal information, politicians and activists have proposed regulation on a number of fronts. Several senators wrote to ask the Federal Trade Commission to investigate whether "the non-consensual compilation, sale, and usage of data-bases" is "a violation of private citizens' civil rights" and whether the databases are "subject to unlawful usage" and "create an undue potential for fraud on consumers."[23]

Currently, consumers have the right to opt out of list sales, though few exercise it.[24] Some privacy advocates favor a rule, the opt-in rule, that requires consumers to explicitly consent to the collection and transfer of information about themselves.[25] A similarly restrictive rule has been adopted by the European Union, whose member countries must comply with it by 1998.[26]

On January 7, 1997, Rep. Bruce F. Vento (D-Minn.) introduced the Consumer Internet Privacy Protection Act of 1997 (H.R. 98).[27] The bill states that "an interactive computer service shall not disclose to a third party any personally identifiable information provided by a subscriber to such service without the subscriber's prior informed written consent." The bill defines "written consent" narrowly, as "a statement--

(A) in writing and freely signed by a subscriber;

(B) consenting to the disclosures such service will make of the information provided; and

(C) describing the rights of the subscriber under this Act."

Many web sites now obtain the consumer's consent by e-mail registration form; the bill would outlaw that practice; online business would be clumsily interrupted by a paper and postage

requirement. Furthermore, online services would be required to provide an express opt-out for subscribers at any time.[28] The bill would empower the FTC to investigate violations of the act and issue cease and desist orders.

Rep. Billy Tauzin (R-La.) has also introduced legislation to create new privacy rights on the Internet. The Data Privacy Act of 1997 requires the interactive computer service industry to develop guidelines as to how they will notify consumers before collecting any "personally identifiable information."[29] The guidelines would require the industry to allow consumers to track the transfer of their personal information to third parties and to obtain the consent of consumers before disclosing that information. The bill contains additional restrictions on collection of information from children,[30] and to allow consumers to opt out of the network of personal information collection and transfer to third parties.

Other proposals to establish mandatory opt-in would not directly involve congressional action but would instead rely on a variety of types of industry "self-regulation."[31] Former FTC commissioner Christine Varney favored "voluntary systems of standards or ratings, whether for privacy or content . . . backed up with strong government enforcement against misstatement as either deception or fraud."[32]

Note, however, that if regulators threaten to punish those who do not "self-regulate" as expected, "self-regulation" becomes government regulation by another name.[33] National Telecommunications Information Administration chief counsel Barbara Wellberry says, "We favor self-regulation, but self-regulation with teeth. But people say self-regulation, and that's the end of the conversation. We're looking at self-regulation more analytically: to see where it works, where it may not work."[34] This level of scrutiny of the industry hardly qualifies as deregulatory, whether one calls it "self-regulation" or not.

Some privacy advocates favor even more heavy-handed regulation, such as the creation of a federal privacy agency or office or special protections for children.[35] Departing from its professed commitment to industry "self-regulation," the FTC itself recently ruled it would "likely be an unfair practice" for a Web site to collect "personally identifiable information such as name, e-mail address, home address or phone number, from children and sell or otherwise disclose such identifiable information to third parties without providing parents with adequate notice . . . and an opportunity to control the collection and

use of the information."[36] Because, as recognized in the recent court challenges to the Communications Decency Act, it is very difficult or impossible for Web sites to identify the age of visitors, the FTC decision might have far-reaching implications for adults as well. There is no First Amendment objection to true self-regulation, that is, industry self-regulation without the threat of government involvement. By contrast, mandatory opt-in, enforced by direct or indirect regulatory pressure, makes no moral sense and would do real economic harm.

The Conflict between Privacy and Free Speech

Cordoning off information behind a wall of new privacy rights violates principles of free speech, threatening to shrink the total domain of freely flowing information.

Humanity's established freedoms have always included, with only narrow exceptions, the right of human beings to learn about one another. In the course of a single day, an individual collects an enormous amount of information about people he encounters--their age and appearance, their manner of speaking and dressing, and their actions and preferences. Except under rare circumstances, he will feel no obligation to ask anyone's permission before relaying the information he has collected to a third party, however embarrassing that might be to the subject of their conversation ("Did you notice that Bob Jones's suit was absolutely covered with dog hair?").

Journalists have no general obligation to get anyone's permission before writing a story about her activities, even though that story and the details of the person's life that they report may be very personal and are sold for commercial value. Journalists have often used information available over computer networks to develop and track important news stories. The newspaper may be penalized if the information violates copyright laws, is defamatory, or violates other common law rights, but these exceptions are very narrow (and themselves often collide with First Amendment rights of free speech).[37] No general "consent" requirement applies.

Regardless of how one defines privacy, "one aspect of privacy is the withholding or concealment of information."[38] A country that takes the freedom of information seriously cannot properly prohibit one business from communicating information about real events and real people to other businesses. If one buys a lawn mower from Sears, the sale of the lawn mower is an

actual event involving a real person. The view that information such as the purchaser's name, address, and buying habits should not be recorded and transferred without his consent conflicts with the general rule that facts and ideas, including our names and addresses, remain free for all to collect and exchange. Attempts to restrict the transfer of information thus run headlong into our rights to free speech.[39]

The following sections explore the main arguments for overriding free speech rights to create new privacy rights in more detail. Many people learning of the existence of a collection of personal data about themselves feel uneasy.[40] "The notion of having others poke into our lives, record it and sell to their own benefit is ethically disturbing."[41] But creating new privacy rights cannot be justified simply because people feel vague unease.

The Economic Role of Consumer Data Compilation--and Gossip

The creation of an entirely new legal regime is hard to justify under any circumstances. Privacy advocates have tried to justify the creation of a new privacy regime by arguing that consumer databases present a new or unique problem. In making these arguments, however, privacy advocates immediately run into difficulty. There is an obvious similarity between the information collected in databases about consumers and the information we regularly exchange with one another informally ("Mrs. Horton has a new car!"). For the vast majority of people, the casual exchange of this type of information--commonly called "gossip"--is not an evil great enough to justify regulation. So privacy advocates must argue that gossip is fundamentally safer, more trivial, and of much less economic consequence than the new databases. But as the following discussion shows, private-sector databases have consequences similar to those of gossip, can serve the same economic and social functions, are more likely to be accurate, and are less likely to contain errors motivated by malice.

Are Private-Sector Databases Worse Than Gossip?

Advocates of the creation of new privacy rights argue that the compilation of data about consumers does more damage than gossip because it takes place on a larger scale. Brandeis and Warren argued that "as long as gossip was oral . . . [one's]

peace and comfort were . . . but slightly affected by it."[42] The same view is echoed today:

> Twenty years ago, say, the local butcher might know that Mrs. Jones bought a ham every Saturday. That was, in a sense, public information. Yet it was not widely available. Perhaps the butcher let the mustard merchant know about Mrs. Jones; but there was no easy way for just anybody, out of idle curiosity or for any other reason, to find out. This is changing.[43]

Another advocate adds that "new retail distribution of sensitive personal information to the public at large increases the social risk of exposing previously private information to friends, colleagues and enemies."[44]

But one cannot meaningfully distinguish consumer databases from gossip on the grounds that gossip causes no harm. Historically, gossip exchanged within small communities could cause terrible harm indeed, because public commentary within those communities had powerful influence over others' lives. One anthropologist notes that in an isolated Spanish village,

> People live very close to one another under conditions which make privacy difficult. Every event is regarded as common property and is commented upon endlessly. . . . People are virtuous for fear of what will be said.[45]

Returning to the butcher example, if buying ham were considered controversial within Mrs. Jones's religious community, her reputation could suffer great damage. "When individuals are dependent on one another for cooperative hunting, farming, herding, or for access to wage labor, gossip and the reputations it creates can have serious economic consequences."[46]

The collection of such information on a large scale in a ham seller's modern database is less likely to have a harmful impact on Mrs. Jones's life than is gossip, since few of the people who have access to the information will particularly care about Mrs. Jones or have power over her, especially if Mrs. Jones is a typical resident of a large, anonymous urban community. Even if she lives in a small town, the employees of the creator of the database usually will not live anywhere close by.

Commercial compilations of data about consumers are likely to be much more accurate than gossip. Companies in the business

of collecting and selling consumer information, whether it relates to purchasing habits or credit history, have an incentive to sell correct information. Errors will occur, but (in contrast to gossip) those who maintain commercial databases have a concrete profit incentive to get the details right.

Many complaints about private databases surface when people find errors in their credit reports. But the evidence suggests that, on the whole, rates of error in credit reports are low. Two highly publicized but biased studies misleadingly report high rates of error in credit reporting (from 30 to 50 percent).[47] A 1991 study by Consumers Union relied on its own employees and their acquaintances to review their own credit reports and report "inaccuracies." Consumers Union did not check whether those claims of inaccuracy were true or false, however, or try to identify the source of the errors.[48] Ralph Nader's Public Interest Research Group also failed to select a random sample, instead estimating an error rate from a sample of consumers who had paid to review their credit reports--people who probably had reason to suspect they would find errors.[49] A more rigorous study of 15,703 consumers, conducted by Arthur Anderson & Co., showed that the true error rate is probably as low as 1 percent.[50]

Finally, databases of information about consumers tend to be much more impersonal and protective of consumer privacy than gossip. Companies that collect information about consumers carefully protect that information in order to save their investment from competitors. These measures also preserve consumer privacy. When the company sells the use of its list to a direct marketer, it does so through a third-party "fulfillment house." The fulfillment house is in the business of compiling lists, creating mailing labels, and attaching those labels to the mail to be sent out; the marketer does not even see the list or the labels, let alone the information in the files. To preserve its reputation in the industry, the fulfillment house must protect the company's list from disclosure. Companies enforce this by "seeding" the lists with dummy entries, usually fake names and real addresses. If those addresses begin getting mail from competitors, the company knows that the fulfillment house has betrayed the secrecy of its list.[51]

In every respect, then, databases of consumer information are likely to be substantially less harmful than gossip. If we do not regulate the exchange of personal information in private conversation, we cannot justify regulation of consumer databases.

The Social and Economic Function of Gossip and Databases

The preceding section discusses the "harm" of gossip or databases from the perspective of the person being gossiped about or reported on. This section compares the economic function of gossip and databases from the standpoint of the community. From that standpoint, the consequences of gossip or databases might be not harmful but beneficial. If I learn through gossip or a database that the baby sitter I was about to hire is a convicted pedophile or even a TV-watcher with little interest in children, this benefits me, though it "harms" the pedophile or couch potato.

Anthropologists observe that gossip, defined as "informal, private communications between an individual and a small, selected audience concerning the conduct of absent persons or events," holds communities together. In nonliterate societies, gossip can be an important means of storing community history.[52] Gossip serves not only a social but an economic function; in societies where food is scarce, gossip centers around food distribution.[53]

As illustrated by the butcher example above, gossip and other informal personal contacts serve an important function in more advanced economies, such as that of the United States in the 19th century. Entrepreneurs could increase their sales by acquiring information about their customers. Customers relied on their neighborhood banker, known since childhood, to give them credit. They could return again and again to the same stores for personalized service.

Today, however, most residents of the United States can escape neighborhood gossip by moving to the anonymity of the city. Many business exchanges occur between strangers who will never meet again. This has many benefits, as "formal freedoms and growing wealth allow people to flee the oppressive constraints of family, local community, or figures of petty authority, for the anonymity--and anomie?--of life in large metropolitan areas."[54] But the new world of strangers has costs as well, as noted by Adam Smith:

> While a man remains in a country village his conduct may be attended to, and he may be obliged to attend to it himself. . . . But as soon as he comes to a great city, he is sunk in obscurity and darkness. His conduct is observed and attended to by nobody, and he is

> therefore likely to neglect it himself, and to abandon himself to every low profligacy and vice.[55]

Today, informal networks like gossip cannot provide the consumer information entrepreneurs want to use to increase their sales or to process a request for credit.

In the new world of automated commerce, more formal electronic networks will naturally replace gossip. Economists have documented how formal networks for checking credit and assessing the reliability of goods have grown out of informal networks. Dun & Bradstreet, which reports on the creditworthiness of businesses, originated with Lewis Tappan, who managed credit accounts in his brother's silk business and who exchanged letters with 180 correspondents throughout the country about the creditworthiness of businesses in their communities.[56] Forty years ago community-based nonprofit organizations handled consumer credit reporting, now handled by three nationwide for-profit firms.[57]

The evolution of formal information networks such as consumer credit reporting has important benefits for the public as a whole. Even the poor or those who are not well known in a given community may buy on credit, a relatively recent and beneficial development.[58] The existence of credit reports gives consumers an incentive to make payments on time, which means that businesses can lower the losses they suffer from default.[59]

Once, the butcher knew of Mrs. Jones through gossip and direct interaction. Today, he and his competitors learn about consumers from customer profiles, lists, and credit reporting services. The formalization of the collection of information about consumers portends nothing sinister. Databases are a natural entrepreneurial adaptation to a more urban world, freed of small-town gossip.

The Economic Consequences of Mandatory Opt-In

Because trade in consumer information serves an important economic function, regulatory obstacles to collecting this information can have hidden economic costs.[60]

Suppose that policymakers set the default rule for the collection of information such as names and addresses so that consumers had to give their explicit consent to use such information. If a substantial number of customers refused to allow

information about them to be transferred to third parties (or simply did not bother to opt in), lists would cost more or disappear altogether. One article predicts that under an opt-in regime the compilation of information would be taken over by "only a handful of companies with unique brand franchises, strong relationships with their customers, or radically new strategies."[61] Developments in Europe, where regulations strictly limit the transfer of personal information, suggest that a mandatory opt-in regime would nearly wipe out direct marketing.[62]

The mandatory opt-in rule would favor larger and older companies at the expense of newer, smaller ones. Established companies could afford more costly lists more easily than could small companies. And established companies would also have less need for lists, since they would have been in business long enough to collect information on their own. The brunt of an opt-in law would thus be borne by small, new businesses or nonprofits struggling to establish a customer base. In one survey, 27 percent of respondents reported making a donation to a charity or a political cause in response to a mailed request.[63] About the same percentage of the population makes purchases through direct mail.[64] While that is not a majority, it constitutes a significant minority--tens of millions of people.

Under mandatory opt-in, firms that could afford to send direct mail would no longer be able to target it effectively. That would lead to fewer, more expensive options for those who shop at home--the elderly, the disabled, rural residents, and anyone without a car--because their mobility is restricted.

In a world without readily available, cheap marketing lists, it is doubtful that another company like Lands' End would ever be born. Mandatory opt-in could preclude, not only the development of new businesses, but the development of whole new business models and product lines designed to serve groups of customers that could never before be identified. Had mandatory opt-in rules been in place a hundred years ago, for example, consumer credit reporting might never have developed.

Free Speech versus Property Rights in Personal Information

You do not have the right to walk into your neighbor's house and make a political speech without his permission, or to spray paint a poem on the walls of an office building. In that

sense, others' property rights define our rights of free speech. The debate about the creation of new privacy rights must therefore also address property rights.

Opponents of private databases and direct marketing assert that those who collect consumer information steal the information from its rightful owners. One advocate argues that "the value in an individual's name belongs to the individual, celebrity and homeless alike. . . . My name is my property and, without my permission, my life is not for sale,"[65] and urges lawmakers to "forbid any sale of personal information without the permission of consumers. This is easiest done by defining personal information to be the property of consumers."[66]

Others make a similar argument couched in softer terms, that customers should have a "right to choose" whether their information is collected. Under that view, privacy should be an "assignable right."[67] But however one phrases it, the argument that we own information about ourselves has fatal flaws.

The Argument Proves Too Much

First, the argument that information about oneself is property proves too much. If I have property rights in a book or an apple, then I can prevent others from using it, regardless of whether they intend to use the item for purposes of trade or sale or for any other purpose. If personal information such as a name is property, the implication is that the "owner" must give permission for every use or collection of the name, not just commercial uses.

Suppose that I meet someone at lunch, learn his name, notice that he is wearing an expensive blue suit, and observe that he has very bad table manners. After lunch, I relate my observations to a coworker. Since the subject of my comments has not expressly given me permission to notice his characteristics or use his name, the "information is property" argument implies that I have "stolen" the information from him, or at least violated his right to choose what information about himself I will reveal--an absurd result.

One might argue in response that the subject of my comments by meeting me has implicitly given me permission to collect information about him. But if consent can be implied, there is no reason that it should not be implied in the commercial context as well. After all, most people know by now that credit

card companies, for example, exchange marketing and credit information with other companies, and more and more people are aware that online transactions can be recorded. Implied consent thus cannot save the "information is property" argument.

The Value of Consumer Information

One might argue that collection of information in a commercial context is different from collection of information in casual encounters, because the commercial information involves something valuable and the casual exchange of information in everyday encounters does not.

That argument also fails. First, the casual exchange of information about people we encounter on the street and in meetings certainly has value to us, although we might not normally place a dollar value on it.

Second, although commercial information does have monetary value (sellers of mailing lists, for example, typically charge from $.10 to $1.00 per name), the value does not somehow inhere in a person's name. Rather, the activities of marketers and list compilers create the value of the name. The name alone, without the economic activities of others, has little or no commercial value. The individual to whom the name refers has no more right than anyone else to claim that value, and in many cases less.

Third, information about a person's buying habits "belongs to" the person providing the product as well as the person consuming the product. To return to an earlier example, if someone buys a lawn mower from Sears (or asks about lawn mowers on Sears' Web site), two parties engage in the transaction--the customer and Sears. Why should the information about the sale belong only to the customer and not to Sears as well? If the customer were to complain about the transaction to Consumer Reports, he would not have to ask Sears's permission. Why cannot Sears boast of the transaction to its creditors?

Contract, Copyright, and Free Speech

One privacy advocate argues that prohibiting trade in mailing lists will not run afoul of the First Amendment because

> The First Amendment does not allow anyone to trade in someone else's property without permission; it does

> not allow the sale of books without the permission of the author, even one poem in an anthology. Direct marketing companies themselves treat mailing lists as their own property and usually "rent" them for one-time use. If mailing lists cannot be traded without permission when they are the property of the direct marketing companies, they should not be traded without permission when they are someone else's property.[68]

But this argument begs the question of whether we do own information about ourselves. Customarily, we simply do not.

The example of the ownership of books and poems is irrelevant. Books and poems are covered by copyright law, which protects only the author's original expression (her choice of words, phrases, and sentences)--not the facts and ideas that she expresses. One could not copyright the historical facts of the battle at Verdun; likewise, one would not be able to copyright the fact that one bought a lawn mower from Sears.

The example of the restricted resale of marketing lists likewise proves nothing. Once compiled, lists have commercial value, which the compiler preserves by insisting that those who rent a list use it only once. But that restriction is enforceable only against the party who rents the list and agrees to the terms of the contract. The list company could not prevent anyone from compiling the names and information on the list independently. The individual names and facts about those named never become the list compiler's property.

Annoyance Is Not a Moral Imperative

Free speech should be protected even when it annoys. Those who favor the creation of new privacy rights use their annoyance with direct marketing as a justification for regulation. They condemn the collection of consumer information out of fear that the creation of databases of consumer information will result in a deluge of junk mail and phone calls. They argue that direct marketing is somehow "unfair" or promotes consumerism, particularly when marketers target children. But these arguments do not provide a sound justification for government action; consumers face little or no danger from those who merely want to persuade them to buy things.

The Triviality of Concerns with Direct Marketing

Many people complain about the annoyance of direct marketing. One activist states, "Like most people, I receive a lot of 'junk mail' and 'junk calls.' These unrequested mails and telephone solicitations have little value to me. . . . As a consumer, I feel annoyed and defenseless in my own home."[69] Similarly, in asking whether the effort of privacy advocates to raise awareness of privacy issues is "creating a spurious need [for privacy]," Esther Dyson answers, "everything tells us that customers feel more and more bewildered by the array of choices facing them."[70]

But annoyance or confusion cannot provide a moral foundation for pro-privacy legislation. Much that annoys should clearly remain legal. Some are annoyed by whiny children in restaurants, or street merchants and musicians, or repeated requests from neighbors trying to borrow tools. Those who find junk mail annoying may complain loudly, but annoyance does not give anyone a moral imperative to regulate.[71] Both "annoyance" and "confusion" are too trivial and too subjective to supply a moral foundation for the creation of new privacy rights.

First, we differ widely in what we find annoying or confusing. In one survey, 71 percent of 18- to 24-year-olds said they would like to receive mail on products that interested them; 68.7 percent of those aged 65 and over reported they would not.[72] Another survey reported that 52 percent of consumers would be interested in subscriber-profiling activities over interactive networks that resulted in their receiving information about special offers.[73]

Second, responses to survey questions about what is "annoying" or "confusing" may not be the best indication of the value of direct marketing. For example, many respondents may not realize the extent to which they "use" advertising mail from which they <u>do not</u> purchase any items. When I purchase clothing from one catalog, for example, I use similar catalogs to comparison shop. Even the information that certain products <u>do not</u> interest me can prove useful. I know from their direct mail that Neiman-Marcus's clothes are usually out of my price range, and that JC Penney's do not suit my taste. The process of comparison and elimination saves time and money, but it is probably a benefit of junk mail that many people overlook.

Third, the problem of junk mail, on a scale of human concerns, is trivial. We can deal with the annoyance of junk calls during the dinner hour by using caller ID,
screening calls, or just hanging up. We can toss unwanted mail

in the wastebasket. New technology such as anonymous digital cash stored on "smart cards" will help people preserve their privacy in online transactions;[74] "anonymizers" can let people cruise the Internet without revealing their identities.[75]

In other words, we do not need the government to protect us from people and firms collecting information simply in order to offer us goods and services. Consumers face no real danger here.

Marketing to Children Does Not Justify Regulation

But what about children? The argument behind almost every restraint on free speech imposed on the electronic media, from the Communications Decency Act, to the V-chip, to the indecency restrictions on broadcasters, has been that children must be protected. Defenders of free speech quickly dismiss the argument that concern for children justifies restraints on adult freedoms when it comes to content controls on hate speech or speech with violent or sexual content. Ironically, some of the same groups that led the battle against the Communications Decency Act, which limited adult speech on the Internet in the name of protecting kids, are leading calls for government protection of kids in the form of privacy regulation,[76] an inconsistency that borders on hypocrisy.

True, young children cannot distinguish commercial pitches from noncommercial entertainment, especially if no one has tried to explain the distinction to them. And they do have money--or can urge their parents to spend money. That attracts marketers, who have been known to collect information about children from Internet sites.[77] Privacy advocates cite this as a justification for restrictions on the collection or transfer of marketing lists that contain information about children.

But the vulnerability of children is not a unique justification for restrictions on marketing, since myriad other speech activities may influence children. On the Internet, for example, children may encounter Ernst Zundel's assertions about Nazi UFO bases at the South Pole and other bizarre or frightening ideas such as those of the Heaven's Gate cult.[78] Concerned parents should sit down with their children and explain the credibility of Internet pitches. Or they can buy software, like Net Nanny, that prevents their child from giving out information online such as names, addresses, and credit card numbers and that can block hate speech or sexual content.[79] There is no unique need for government to regulate Web site content, whether

that content is commercial or indecent or political.

More fundamentally, do children face any real harm from marketing? The main risk seems to be that children might end up with a little more useless junk than they would have otherwise. This is just not a serious problem. Over time, children might--or might not--learn some valuable lessons from careless consumerism. Many children have been inexpensively educated about the pitfalls of mail order from the "Sea Monkeys" sold in comic books: to children's surprise, brine shrimp do not develop much personality or wear clothing, as the ads suggest.

Compared with most of the world, we live in an affluent society. We not only buy many things for our children, we also give our children their own money to spend. It makes little sense to morally condemn those who sell to children when we ourselves give children the means to buy. So regulation of marketing lists that contain information about children is no more justified than regulation of lists containing information about adults.

Abuse: Access by Criminals

Like other technological tools, private databases can be used for purposes for which they were not intended. A reporter using the name of a convicted child murderer, "Richard Allen Davis," obtained an address list of 5,000 school children from a commercial list seller.[80] A woman was stalked and harassed by a convict employed to enter data in a private database.[81] Does the possibility of undesirables accessing lists justify regulating everyone's access?

To some extent, penalties for procedures that tend to lead to abuses already exist. Irresponsible practices like the hiring of prisoners as data entry clerks leave companies open to lawsuits under the common law for simple negligence.[82] Committing fraud and murdering children clearly remain illegal.

Would the danger of the abuse of lists justify a mandatory opt-in rule? Though such abuse is certainly real and not a trivial matter like "annoyance," mailing lists should not be singled out as the only area of concern. Public libraries contain information about how to make nuclear bombs. Newspapers contain extraordinary amounts of personal information that criminals could use. In one infamous case, an imprisoned pedophile used stories about children from small-town newspapers

to compile a list of 300 potential victims.[83] But such dangers would not justify regulation of newspapers, even though convicts have much greater access to newspapers than to mailing lists. The First Amendment protects free speech, even though that right might be abused.

And one cannot argue that the compilation of information in lists for commercial purposes is different just because it serves a commercial purpose. The content of databases is not "commercial speech," because the lists themselves are not advertising--they are data. And the lists are used for political purposes or for nonprofit solicitations as well as for commercial advertising.

Restrictions on the collection of information for mailing lists, such as a mandatory opt-in rule, thus are classic "prior restraints" on content. The Supreme Court frowns on prior restraints on speech,[84] allowing them only when publication would "surely result in direct, immediate, and irreparable damage to our Nation or its people."[85]

The abuse of mailing lists by stalkers or psychotics cannot justify a wholesale system of prior restraint on mailing lists. These invite abuse no more than other sources of information, such as newspapers or phone books.

Why Government Databases Are Different

Most privacy advocates conflate private and government databases.[86] Some people view private databases as worse than government databases. Leslie Byrne of the Office of Consumer Affairs compares private data collection to Big Brother, saying, "With the possibility of anonymous data gathering, companies have become Big Brother to many. It's more than controlling your life in a sci-fi way; it's selling your life."[87]

But the claim that selling information about someone automatically involves seizing control of that person's life, or worse, cannot survive critical scrutiny. The First Amendment should protect the compilation of information in private databases. But government databases are different and should be tightly restricted. This section explores some of the philosophical distinctions between private and government databases, without attempting to provide detailed support for the more empirical claims that governments would abuse these databases.

Databases and the Constitution

The First Amendment protects citizens' rights to compile information in databases, just as it would protect their right to collect it in a diary or a book. Nowhere does the Constitution restrain the powers of private citizens to collect information. By contrast, some provisions of the Constitution, such as the Fourth Amendment, do constrain the power of government to interfere in our lives and collect information about us, consistent with the fundamental purpose of the Constitution to define and limit the power of government. The drafters of the Constitution saw government as a necessary evil and so established a system to limit the government's powers to those they had explicitly enumerated.

It is generally assumed that private citizens are permitted to take any action that law does not explicitly forbid, whereas the government is generally forbidden to take any action that the Constitution does not allow. Thus, restrictions on private data collection violate First Amendment protections of free speech, whereas restrictions on government databases or on government access to existing private databases simply fulfill the promise of the Fourth Amendment.

The Unique Danger of Government Abuse

Although both private and government databases can be abused, the abuse of government databases poses a more serious threat for one reason: government controls the courts, the police, and the army. Marketing agencies compile lists primarily to sell us things--a nuisance, perhaps, but little more than that. Governments compile lists primarily to enforce the law. Because the state claims so much more power than private parties--power that it then abuses--government databases pose terrible risks.

We can protect our privacy from private marketers by not getting credit cards or not ordering from catalogs. We can have our names removed from marketing lists. We can buy software to stop our kids from giving out information on the Internet. We can scream obscenities at direct marketers who call during dinner. But we dare not do that to the Internal Revenue Service. In the course of enforcing tax, highway, and public health regulations, the government has far more power to collect information than any private company, and more power to act on that information once it is collected.

Recent abuses of government databases demonstrate the danger. A Florida health worker distributed lists from a health database of AIDS patients in bars so the patrons could screen sexual partners.[88] In Oregon, someone posted on the Internet a copy of state Department of Motor Vehicles records available for sale from the state for $222, enabling anyone to match a vehicle license number with the vehicle's registered user.[89] In California, where Department of Motor Vehicles records were available on request, a stalker used them to locate and murder actress Rebecca Shaffer. A recent investigation of the IRS revealed the troubling tendency of its employees to snoop around in the agency's files to learn about their acquaintances' finances. The recent leaks of Federal Bureau of Investigation files to the White House provide another notorious example.

Interaction between Private and Government Data Networks: Social Security Numbers

The government creates special problems by assigning to every American citizen a universal identifying number, a Social Security number. Because no one can "opt out" of having a Social Security number, private-sector data collectors will inevitably use these numbers as universal identifiers for nontax purposes. In 1996 there was a public outcry when P-TRAK, which maintains a database available through LEXIS-NEXIS, announced its plan to include Social Security numbers in its database.[90]

If we view private databases as fundamentally different from government databases, how should we view the private use of government-mandated identifying information? The widespread use of Social Security numbers as identifiers is a consequence of allowing a government data collection process to get out of control and develop uses it was never intended to serve. Social Security administrators should be restricted from releasing information about Social Security numbers to other agencies or to private parties, and state and local governments should be prevented from using these numbers on driver's licenses and other official documents.

Other restrictions on the proliferation of these numbers, such as prohibiting businesses from requiring customers to provide Social Security numbers, might also be appropriate. However, it is hard to see how all private uses of Social Security numbers could or should be prevented. If it is not unreasonable for gas stations to record the license number of a car making a purchase of gas on credit, it is arguably justifiable

for credit reports, for example, to contain identifying information such as Social Security numbers.

The long-term answer may be to limit the state's power to intervene in our lives; if, for example, the Social Security system were privatized, there would be no need for universal Social Security numbers.

Conclusion

As we go about our day-to-day affairs, we collect and process an enormous amount of information. This process is so natural and necessary to our lives that we take it entirely for granted. We see it as a serious threat only because advanced telecommunications technology lets us wander about the world in new, automated ways, and we realize that the collection of information has become mechanized as well. It is a mistake to view the collection of information as morally shocking simply because we have never noticed that it goes on.

Any law that restricts the compilation of information endangers free speech. Laws that make it more difficult and expensive to compile databases have a disproportionate impact on small and new businesses that cannot afford other means of growing.

The supposed "moral" justifications for restricting the compilation of customer information by private companies do not make sense. The main impulse behind the pro-regulation forces seems to be that commercial exchanges are somehow ignoble or wrong, a sentiment out of place in a country that owes so much to free enterprise.

We should focus our concerns about privacy on the dangers posed by government databases, not private databases. The danger to our civil liberties from government databases is vastly greater.

Notes

1 http://www.theonion.com/onion3213/indes3213.html, October 30, 1997.

2 Albert B. Crenshaw, "Companies' Consumer Data Makes More People Uneasy," Washington Post, November 5, 1995, p. H1.

3 See Louis Harris & Associates and Alan F. Westin, "Commerce, Communication and Privacy Online: A National Survey of Computer Users," study conducted for Privacy & American Business, 1997. Over 70 percent of 9,300 consumers who responded to an online survey are more concerned with privacy on the Internet than about information transmitted by phone or mail. eTRUST, "Survey Reveals Consumer Fear of Privacy Infringement Inhibits Growth of Electronic Commerce," News Release, March 24, 1997, p. 1.

4 Steven E. Miller, Civilizing Cyberspace: Policy, Power and the Information Superhighway (New York: Addison-Wesley, 1996), p. 265.

5 See "Privacy Profile," Privacy & American Business, October-November 1996, p. 5.

6 Jim Castelli, "How to Handle Personal Information," American Demographics, March 1996, p. 1.

7 This paper does not illustrate this point in detail, saving it for another day. Nazis used census data in Germany, Holland, and Romania to track down and eliminate "undesirables."

8 "Rights to privacy are valid claims against unauthorized access that have their basis in the right to authorize or decline access. These rights are justified by rights of autonomous choice . . . expressed in the principle of respect for autonomy. In this respect, the justification of the right to privacy is parallel to the justification of the right to give an informed consent." Tom Beauchamp and James Childress, Principles of Biomedical Ethics, 4th ed. (New York: Oxford University Press, 1994), p. 410; see also p. 406 (defining privacy as "a state or condition of physical or informational inaccessibility").

9 See, for example, Andrew L. Shapiro, "Privacy for Sale: Peddling Data on the Internet," Nation, June 23, 1997, p. 11.

10 For a variety of sweeping and ambiguous definitions of privacy, see U.S. Congress, Office of Technology Assessment, Protecting Privacy in Computerized Medical Information, OTA-TCT-576 (Washington: Government Printing Office, 1993), pp. 1-3.

11 There was one narrow exception originating in the canon law, the law of libel. See David W. Leebron, "'The Right to Privacy's' Place in the Intellectual History of Tort Law," Case Western Reserve Law Review 41 (1991): 769-809; but see the discussion of the origins of the law of libel and slander in Dorothy J. Glancy, "The Invention of the Right to Privacy," Arizona Law Review 21 (1979): 1-39.

12 See Note, "The Right to Privacy in Nineteenth Century America," 94 Harvard Law Review 94 (1981): 1892-1910.

13 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review 4 (1890): 195.

14 Glancy, p. 6.

15 These include the authors' account of defamation law, which they use to support the idea that the creation of property rights in information was a natural legal evolution. The authors ascribe the origins of the law of libel and slander to the increasing value of reputation among men, and the corresponding need for legal protections. But this theory is little more than speculation. The law of defamation actually arose from canon law concerning the sin of telling a falsehood. The idea was next seized on as an instrument of censorship by the infamous Star Chamber, which brought charges of defamation against critics of the government. Fowler V. Harper, Fleming James, and Oscar Gray, The Law of Torts (Boston, Mass.: Little, Brown, 1986) sections 9.5-9.7.

16 See William Dean Prosser, "Privacy," 48 California Law Review 48 (1960): 383-96; Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905). The torts, some or all of which some states have refused to recognize, include misappropriation of one's name and likeness for commercial purposes, public disclosure of embarrassing private facts, publicly placing the plaintiff in a false light, and intrusion into the plaintiff's seclusion.

17 These include the "right of publicity" laws, which primarily serve sports figures and movie actors trying to ensure that they have a monopoly on the distribution and sale of their own images. See Restatement (Second) of Torts (St. Paul, Minn.: American Law Institute Publishers, 1976) § 652C.

18 See Thomas I. Emerson, "The Right of Privacy and Freedom of the Press," 14 Harvard Civil Rights-Civil Liberties Law Review 14 (Summer 1979):329-60.

19 For example, to succeed in a suit for intrusion into plaintiff's seclusion, one must show an intentional invasion, "physical or otherwise, upon the solitude or seclusion of another or upon his private affairs, or concerns . . . if the intrusion would be highly offensive to a reasonable person." And such suits succeed only if the person has a reasonable expectation of privacy.

20 See the Center for Democracy and Technology's site at http://www.13x.com/cgi-bin/cdt/snoop.pl.

21 Esther Dyson, "Labels and Disclosure Part II: Privacy," Release 1.0, February 19, 1997, p. 17.

22 "American Survey: We Know You're Reading This," The Economist, February 10, 1996, p. 27; see also "Virtual Privacy," The Economist, February 10, 1996, p. 16.

23 Sens. Richard H. Bryan (D-Nev.), Larry Pressler (R-S.Dak.), and Ernest F. Hollings (D-S.C.), letter to the Honorable Robert Pitofsky, Federal Trade Commission, October 8, 1996, p. 1.

24 Information Infrastructure Policy Committee, Draft for Public Comment: Option for Promoting Privacy on the National Information Infrastructure (Washington: National Information Infrastructure Task Force, April 1997), p. 46 (hereafter cited as IIPC Draft).

25 See, for example, Ram Avrahami, "The Market in Personal Information: Analysis, Concerns and Proposed Solution," September 1996 (paper on file with the author).

26 "Virtual Privacy," p. 16; see also IIPC Draft, pp. 4-5 (under the EU approach, personal data may be processed only if the data subject has consented "unambiguously").

27 "Consumer Internet Privacy Protection Act," 105th Cong., 1st. sess., Congressional Record 143, no. 1, (January 7, 1997): E8.

28 Information services would be prohibited from knowingly distributing false information about users. A service would have to give subscribers free access to the information kept about them for correction, as well as the name of any party requesting the information.

29 Data Privacy Act of 1997, H.R. 2368 (1997).

30 The "voluntary" guidelines would require service providers who collect information from children online to first obtain their parents' consent.

31 See, for example, Dyson, p. 2.

32 Ibid., p. 14 (quoting Varney).

33 "The underlying question faced by eTRUST . . . is whether they can successfully garner industry support without the heavy threat of government regulation behind them. In short, can they raise the issue's visibility enough to get the public to care about it and Web sites to self-regulate but still not provoke a government-mandated/controlled system? . . . eTRUST, P3 and efforts like them rarely work without a 'hammer.' . . . Adoption is a long walk through the mud unless you have some externally applied sense of urgency. . . . That's not necessarily just the government . . . but the threat of government action may well promote urgency in other sectors." Ibid., pp. 2, 14 (partly quoting

Andy Blackburn of the Boston Consulting Group, quotations omitted).

34 Ibid., p. 14.

35 See IIPC Draft, pp. 54-68.

36 http://www.ftc.gov/os/9707/cenmed~1.htm, July 18, 1997.

37 See New York Times Co. v. Sullivan, 376 U.S. 254 (1964) (newspaper may be held liable for defamatory statement against public official only if plaintiff proves the statement was made with "actual malice"); Cox Broadcasting v. Cohn, 420 U.S. 469 (1975) (newspaper may publish rape victim's name once it is a matter of public record); Time, Inc. v. Hill, 385 U.S. 374 (1967) (magazine cannot be liable for inaccurate portrayal of an individual's private life unless the plaintiff establishes knowing or reckless falsehood); Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979) (state law punishing truthful publication of the names of juvenile offenders violates First Amendment); see also Harper & Row, Publishers, Inc. v. National Enterprises, 471 U.S. 539 (1985) (magazine's right to publish extensive quotations from leaked manuscript in violation of copyright law not protected by First Amendment).

38 Richard A. Posner, "An Economic Theory of Privacy," Regulation, May-June 1978, p. 19.

39 One implication of the recent draft policy report by the Information Infrastructure Policy Committee is that effective enforcement of privacy rights might require limitations on anonymous speech. See IIPC Draft, p. 7.

40 Some 80 percent of Americans report that they worry that they have "lost all control" over their personal information. "But at the same time they are extraordinarily willing to fill out warranty cards, questionnaires and impertinent surveys." "American Survey," p. 28.

41 Ram Avrahami, "Privacy Petition," February 1997, p. 1 (on file with the author).

42 See Brandeis and Warren, p. 217 n. 48.

43 "Virtual Privacy," p. 16.

44 Avrahami, "The Market in Personal Information," p. 4.

45 Sally Engle Merry, "Rethinking Gossip and Scandal," in Reputation: Studies in the Voluntary Elicitation of Good Conduct, ed. Daniel B. Klein (Ann Arbor: University of Michigan Press, 1997), p. 47 (quoting a study of an Andalusian town).

46 Ibid., p. 59.

47 Daniel B. Klein and Jason Richner, "In Defense of the Credit Bureau," Cato Journal 12 (Fall 1992): 402-7, discussing Consumers Union study "What Are They Saying About Me," April 29, 1991; see also Edmund Mierzwinski, "Nightmare on Credit Street or How the Credit Bureau Ruined My Life," Report, United States Public Interest Research Group, June 6, 1991.

48 Klein and Richner, pp. 403-4.

49 Ibid, pp. 405-7. The PIRG study also failed to identify the source of the errors and reported anecdotes featuring consumers' unconfirmed assertions that their reports contained errors.

50 Ibid., pp. 407-8.

51 Peter Vanderschraaf, California Institute of Technology, letter to Professor Dan Klein, University of California at Irvine, June 23, 1995, p. 1. Copy in author's files.

52 Merry, p. 50.

53 Ibid., p. 54.

54 Jeremy Shearmur and Daniel B. Klein, "Good Conduct in the Great Society: Adam Smith and the Role of Reputation," in Reputation, p. 29.

55 Adam Smith, quoted in ibid., p. 34.

56 Daniel B. Klein, "Knowledge, Reputation, and Trust by Voluntary Means," in Reputation, p. 7.

57 Ibid.

58 Using credit is safer and more convenient than paying cash. It also gives the consumer more flexibility in adjusting his purchases to his earning schedule. He can finance large purchases such as a home by spreading the payments out over his entire life. Klein and Richner, pp. 394-95.

59 Ibid., pp. 395-96.

60 Implicit in the argument that "customers should be able to choose" whether their information will be included in databases or not is the argument that giving them the right to choose would do little harm. Esther Dyson says we should

> consider the work of economist Ronald Coase, who won the Nobel Prize for this insight among others.

> If you establish a right--whether it's for clean air, privacy, a pound of potatoes or a copy of a newsletter--that right will be allocated efficiently in a free market, regardless to whom the right is initially assigned.

Dyson, p. 4. One implication of this might be that changing the default rule from opt-out to opt-in would make little difference in the ultimate economic outcome. But Dyson has Coase's observation wrong. Coase's observation held only in a market where transaction and information costs--the costs to the property owners of learning about opportunities and trading their rights--are zero--that is, in one (imaginary) type of free market, not in all free markets. Obviously, in the real world, transaction and information costs are not zero. In the real world, then, it matters very much when the default rules are changed from opt-out to mandatory opt-in.

61 John Hagel III and Jeffrey F. Rayport, "The Coming Battle for Customer Information," Harvard Business Review, January-February, 1997, p. 54. The opt-in system these authors describe would be enforced by technology rather than by law. But the outcome of an opt-in system enforced by law would probably favor a few collectors even more strongly.

62 Ibid., p. 5, quoting Pat Faley of the Direct Marketing Association; see also Robert Vastine, "Battling over Data Privacy," Journal of Commerce, July 30, 1997, p. 8A.

63 Beth Negus, "Consumers Nervous about Privacy," Media-Central, June 17, 1996, p. 1.

64 Ibid.

65 Ram Avrahami, "My Name Is Not for Sale," Los Angeles Times, February 5, 1996, p. B5.

66 Ram Avrahami, "Privacy Petition-Background Information," February, 1997, p. 2 (on file with the author).

67 Dyson, p. 4.

68 Avrahami, "The Market in Personal Information," p. 18.

69 Avrahami, "My Name Is Not for Sale."

70 Dyson, p. 16.

71 Indeed, perhaps the most annoying aspect of junk mail is that direct mail operations do not know enough about consumers. One is bound to be annoyed, for example, by calls trying to sell auto club memberships if one does not have a car. Thus, restricting the collection and transfer of personal consumer information may actually increase the proportion of unwanted junk mail by hindering targeted marketing.

72 Negus, p. 1.

73 National Telecommunications and Information Administration, Privacy and the NII: Safeguarding Personal Information (Washington: Department of Commerce, 1995), p. 25.

74 Hagel and Rayport, p. 58.

75 See http://www.anonymizer.com, March 17, 1997 ("Because on today's Internet, people do know you're a dog"); see also "On the Internet, Nobody Knows You're a Dog," New Yorker, July 5, 1993, p. 61.

76 Julie DeFalco, "Government-Approved Privacy on the Net," Investor's Business Daily, February 27, 1997, p. A32.

77 See Center for Media Education, "Web of Deception: Threats to Children from Online Marketing," April 16, 1997, http://epn.org/cme/pr970306.html.

78 See http://www.webcom.com/ezundel/english, March 17, 1997; see also http://www.envirolink.org/arrs/gallery/gallery.html (animal rights site showing dead greyhounds in a dump and other disturbing pictures), March 17, 1997; see also http://www.contrib.andrew.cmu.edu/~fcca (site dedicated to "Our Lord Jesus the Abortionist"), March 17, 1997.

79 Solveig Bernstein, "Beyond the Communications Decency Act: Constitutional Lessons of the Internet," Cato Institute Policy Analysis no. 262, November 4, 1996, pp. 28-29.

80 "Privacy in Cyberspace," Washington Post, September 2, 1996, p. A22; "Metromail Stung Again," Privacy Times, May 17, 1996, p. 4.

81 In the spring of 1994 Beverly Dennis filled out a questionnaire promising coupon savings. In June of 1994 she got a threatening, obscene letter from a rapist serving time at Wynn Prison. A company had contracted with the prison to process the questionnaires. "Class-Action Suit Targets Companies' Use of Prisoners," Privacy Times, May 17, 1996, pp. 5-6; Nina Bernstein, "Personal Files via Computer Offer Money and Pose Threat," New York Times, June 12, 1997, p. A1.

82 The exact outcome of such a case is hard to predict in the absence of precedents on point. I was unable to discover any such suits prior to the Beverly Dennis case, which has not yet been adjudicated. See Dennis v. MetroMail Corporation, Cause no. 9604451, Plaintiff's Third Amended Class Action Petition for Damages, Injunctive and Other Equitable Relief (District Court for Travis County, Tex.), March 28, 1997.

83 CBS Evening News, November 26, 1996, transcript from Burrelle's Information Services; see also "A Pedophile Keeping Lists," Privacy Journal, December 1996, p. 1.

84 Near v. Minnesota, 283 U.S. 697, 713 (1931). It is for this reason that the Court has held: "Any prior restraint on expression comes to this Court with a 'heavy presumption' against its constitutional validity." Organization for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971) (citations omitted); New York Times Co. v. United States, 403 U.S. 713, 714 (1971)(denying injunction to prevent publication of the Pentagon Papers).

85 In New York Times Co., 403 U.S. at 714, the Supreme Court invalidated a prior restraint on classified material that had been enjoined in the interests of national security. According to Justice Stewart, prior restraints would be allowed only in time of war, and only when disclosure would "surely result in direct, immediate, and irreparable damage to our Nation or its people." Ibid. at 730 (Justice Stewart and Justice White concurring).

86 See, for example, David L. Bazelon, "Probing Privacy," Gonzaga Law Review 12 (1977): 587-619; Brandeis and Warren, pp. 195, 205 (describing privacy loosely as the "right to be left alone").

87 "Privacy Profile," p. 5.

88 "Theft of AIDS Database Prompts New Effort to Guard Information," Washington Times, October 14, 1996, p. A8.

89 "On-Line Databases Draw Privacy Protests: Unfounded Lexis-Nexis Report Reflects Worry about Growing Files," Washington Post, September 20, pp. A1, A7.

90 Lexis is the service used by lawyers and law enforcement agencies to locate witnesses or other parties across the country. The database, known as the P-TRAK Person Locator, contains information such as an individual's maiden name (not the mother's maiden name) or other names, telephone numbers, and up to two previous addresses. A user can type in a Social Security number and find its owner. Thomas E. Weber, "FTC Is Seeking New Safeguards after Lexis Flap," Wall Street Journal, September 21, 1996, p. B7.

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering

proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress.

 Printed Copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write to: Cato Institute, 1000 Massachusetts Avenue NW, Washington, DC 20001.

(202) 842-0200, FAX (202) 842-3490 E-mail cato@cato.org