

PROTECTING CONSUMER PRIVACY: THE ROLE OF OPT-IN

Idaho Legislature Interim Committee on Transfers of Personal Information
Boise, ID, October 4, 2000

Fred H. Cate¹

Privacy is a complex and often emotional issue, and made all the more so because of:

- ▶ its importance to all of us (after all, who doesn't want privacy?)
- ▶ everyone thinks we understand privacy,
- ▶ most people regard privacy as an unmitigated good: if a little is good, more will be even better,
- ▶ it is a broad term that encompasses many tangential or even unrelated issues and concerns—about the proliferation of information technologies, genetic profiling, manipulation, identity theft, fraud, the government accessing personal information, being caught lying to the government or businesses, globalization, aggressive marketing tactics, recent successes of hackers and computer viruses, and a general sense of loss of control.

Privacy issues are even more difficult because privacy is always in tension with other important values and the benefits that flow from open information flows. Proponents of greater government privacy protection often characterize the issue as consumer vs. business. This is not merely inaccurate, but it misses the point entirely about the role of information and privacy in our modern economy. Information is the lifeblood of our 21st century economy. As a result, *restricting information flows to protect privacy always, inevitably imposes costs on consumers, businesses, and the economy as a whole.* Consumers' desire for greater privacy is in tension with our desire for other benefits, such as convenience and low cost, that privacy protection inherently interferes with.

I would like to take a few minutes to suggest just how great this tension between privacy and the benefits that flow from open information flows really is by outlining some of the key uses of routinely shared personal information today. Then I will turn specifically to the issue of opt-in legislation, and finally conclude with some brief recommendations.

Benefits of Information-Sharing

First, the beneficial uses of personal information. I will outline seven:

¹Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington; Senior Counsel for Information Law, Ice Miller Legal & Business Advisors, Indianapolis, IN; Visiting Scholar, American Enterprise Institute, Washington, DC.

1. Information is used to identify and meet customer needs. One of the key attributes of the our economy and the source of the remarkable growth in productivity during the past decade is the application of information technology to help businesses identify and meet consumer needs. Federal Reserve Board Governor Edward Gramlich put it this way in testimony before Congress in July 1999: “Information about individuals’ needs and preferences is the cornerstone of any system that allocates goods and services within an economy.” The more such information is available, he continued, “the more accurately and efficiently will the economy meet those needs and preferences.”² In short, information-sharing allows businesses to ascertain customer needs accurately and meet those needs rapidly and efficiently.

2. Information-sharing also expands consumer access to a wide range of affordable services and products and significantly reduces the cost of many products and services.

For example, because widely available consumer information allows manufacturers, wholesalers, and retailers to know what to make, what to stock, and when, it reduces the cost at which goods and services can be provided to consumers.

In addition, the sharing of reliable, centralized, and standardized consumer information also makes it possible to reduce the cost of providing a variety of means by which consumers can pay for the products and services they want. Such information is the very foundation of consumer credit from banks and retailers, instant credit at point of sale, and many deferred payment programs. Moreover, shared personal information also reduces the cost of products and services by reducing the risks of accepting checks and other non-cash payments.

Information-sharing also allows organizations to outsource many basic business operations to third parties who perform these operations on their behalf. Many businesses outsource marketing, account management, customer satisfaction surveying, and other activities to third parties that specialize in these activities and maintain the infrastructure necessary to perform them efficiently and accurately. These relationships are not always obvious. For example, many retailers provide specialty services and products, such as fine jewelry, photographic studios, vision services, or hair care, through independent companies that license the retailer’s name, but are not the retailer’s affiliates. These independent companies provide services to customers under the retailer’s name, accept the retailer’s credit card, include information and coupons in the retailer’s mailings and advertisements, participate in the retailer’s loyalty programs, and, from a customer perspective, are simply another department of the retailer’s operations. However, because of the nature of the service, efficiencies that come with specialization, insurance factors, and federal and state tax and licensure laws, it is often necessary and desirable for the retailer to provide the service by contracting with a separate company. For smaller companies, outsourcing is what makes it possible for them to compete with established firms and thereby gain the benefits of economies of scale.

²Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of Edward M. Gramlich).

3. Routine information sharing also expands the ability of consumers to take advantage of new products and services. Consumer credit markets provide a case in point. The current U.S. economic boom has significantly raised the standard of living for U.S. citizens through the availability of over \$5 trillion in outstanding mortgages and other consumer loans. The “almost universal reporting” of personal credit histories (under the rules of the Fair Credit Reporting Act) is, in the words of economist Walter Kitchenman, the “foundation” of consumer credit in the United States and a “secret ingredient of the U.S. economy’s resilience.”³ Studies have shown that the comprehensive credit reporting environment in this country has given U.S. consumers access to more credit, from a greater variety of sources, more quickly, and at lower cost than consumers anywhere else in the world. It also reduces the cost of that credit, in the case of mortgages alone, by \$80 *billion* a year.

More complete, reliable, and widely available personal information also has increased the number of Americans who now qualify for credit and other services, and increased the confidence of service providers in meeting the needs of this previously underserved population. In 1956 about 24 percent of U.S. households (13 million) had mortgage loans. By 1998 over 43 percent of households (44 million) had home mortgage loans, and the percent of the U.S. population owning their own homes were at an all-time high.

Lenders, retailers, cable television companies, public utilities, and other businesses use personal information to verify information about new customers. This is particularly important in our highly mobile and increasingly global society. In short, information-sharing facilitates consumer mobility and creates a democratization of opportunity.

4. Information-sharing enhances customer convenience and service. For example, information-sharing greatly enhances the speed with which decisions can be made. In 1997, 82 percent of automobile loan applicants received a decision within an hour; 48 percent of applicants received a decision within 30 minutes.⁴ Many retailers open new charge accounts for customers at the point of sale in less than two minutes, provided that the customer shows appropriate identification. This is unheard of outside of the United States. In other countries, restrictive laws often prevent credit bureaus and other businesses from routinely collecting information from many sources on myriad aspects of consumer activities to maintain the accurate, up-to-date files necessary to support rapid and accurate decision making.

Information-sharing across companies allows a customer to use a store charge card at a jewelry counter or other specialty service provider that is housed, but not owned, by the store issuing the card, and to call a single 800-number to access a variety of accounts and services.. New restrictions on information-sharing make it both more difficult—in some cases impossible—and more expensive for most businesses to provide customers with the type of convenient, efficient service they have come to expect.

³Walter F. Kitchenman, U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns 1 (The Tower Group 1999).

⁴1998 Automobile Finance Study, Consumer Bankers Association, Arlington, VA, at 19.

5. Information-sharing allows consumers to be informed rapidly and at low cost of those opportunities in which we are most likely to be interested. Once a business has developed a new product or service, it must inform potential customers. The cost of alerting consumers about a new product or opportunity can be a major obstacle to the launch of new businesses and prevent innovative products from ever reaching the marketplace. Information technology has made possible targeted marketing whereby organizations use information from a variety of sources to identify potential new customers. “Target marketing” allows a business to send an offer to a customer specifically identified as likely to be interested. In the absence of information that indicates which consumers are likely customers, businesses must choose between marketing randomly, contacting everyone in an entire geographic community, or relying solely on mass media advertising to reach potential customers.

In a nation with over 100 million households, target marketing reduces the prices that consumers pay for products because it dramatically reduces the cost of soliciting customers by raising the likelihood that the consumer receiving the message will actually be interested in the service or product. Businesses must advertise, whether or not they have information about who is likely to be a customer. Targeted marketing reduces those advertising costs relative to mass marketing. Target marketing also reduces the volume and cost of so-called junk mail and enhances consumer satisfaction. We love to complain about junk mail and telephone calls, but in 1998, more than two-thirds of U.S. consumers—132 million adults—took advantage of direct marketing opportunities and convenience, accounting for more than \$1.3 trillion in sales of goods and services.

6. The target marketing made possible by information-sharing is an especially critical resource for new and smaller businesses—the foundation of economic growth and new jobs. It gives them a more cost-effective means to communicate with consumers unfamiliar with their brand name but likely to be interested in their services or products. Targeted marketing, based on personal information obtained from in the market, allows new or small companies which lack extensive customer lists of their own or the resources to engage in mass marketing to reach customers likely to be interested in their products or services.

Interfering with the availability of that information hurts both consumers, who miss out on opportunities, and businesses, who face higher costs to reach consumers, but such interference imposes an especially heavy burden on small companies, which cannot afford mass market advertising and lack the customer lists of their well-established competitors. Open access to third-party information and the responsible use of that information for target marketing is essential to leveling the playing field for new market entrants. Just look at the marketing practices of companies like America Online, which achieved its current status as the Internet’s largest service provider because, as a start-up company, it mailed free copies of its software to people likely to be interested in Internet access. Prohibiting that activity would have denied consumers information about an opportunity that many of them obviously value and AOL access to a market it wished to serve.

Similarly, small businesses, often family-owned, offering specialized products and services rely on accessible information to help them identify and reach those customers, often

thousands of miles away, most likely to be served by their offerings. How else is a company specializing in high-end pianos, or parts for early production Fords, or rare mystery books, or lower-cost supplies for diabetics expected to reach the customers who most need their offerings than through targeted marketing? Many businesses in today's markets never see their customers because transactions are conducted exclusively over the telephone, Internet or through the mail. These businesses are able to identify and reach potential customers they've never met because of the free flowing information that signals that a particular consumer may have an interest in a product. In a global market, information-sharing is key to connecting far-flung customers and businesses.

7. One final example of a key use of personal information is to prevent and detect fraud. More than 1.2 million worthless checks are cashed at retailers, banks, and other U.S. businesses every day, accounting for \$12.6 billion in losses. Treasury Department officials estimate credit card fraud losses to be between \$2 billion and \$3 billion in 2000. The insurance industry paid \$20 billion in 1999 for fraudulent property and casualty claims. Across the economy, business losses due to all forms of document fraud and counterfeiting exceed \$400 billion—6 percent of annual revenue of American businesses—per year. Although businesses covered virtually all of these losses, these losses ultimately affect consumers through higher prices, inconvenience, and lost time and productivity.

Personal information is one of the most effective tools for stemming these losses. Such information is used every day to identify consumers cashing checks and seeking access to accounts. Not only does that information help identify the perpetrators of financial fraud, it also gives retailers and check-cashing services the ability and confidence to accept checks, especially from out-of-state accounts. Close monitoring of account activity also allows credit providers and other businesses to recognize unusual behavior that may indicate that a credit card or debit card has been stolen or is otherwise being used without authorization. Moreover, because of information-sharing, an alert about a lost or stolen credit or debit card can be rapidly shared with other businesses. Similarly, companies share information about fraud schemes and unauthorized account activity so that they can prevent further losses and improve the odds of apprehending the thief.

The benefits of being able to identify and locate specific individuals or groups of individuals are not limited to commercial contexts. Personal information—often aggregated by commercial service providers—is essential to preventing, detecting, and solving other crimes as well. In 1998 the FBI alone made more than 53,000 inquiries to commercial online databases to obtain a wide variety of personal information. According to Director Louis Freeh, “Information from these inquiries assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning.”⁵

⁵Hearings before the Subcomm. for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the Comm. on Appropriations, U.S. Senate, 106th Cong., 1st Sess. (March 24, 1999) (statement of Louis J. Freeh).

Personal information is also used to improve public welfare. Personally identifiable information is used to locate and contact missing family members, heirs to estates, pension fund beneficiaries, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. The Association for Children for Enforcement of Support reports that information provided through commercial vendors helped locate over 75 percent of the “deadbeat parents” they sought. Accessible personal information also helps identify victims of fraud or environmental hazards, and saves lives by locating owners of recalled automobiles and blood, organ, and bone marrow donors. These socially valuable uses don’t pay for the collection and aggregation of personal information; if you restrict those other beneficial uses of personal information that do foot the bill, you eliminate the ancillary benefits as well.

These seven categories of benefits that flow from routine information-sharing are illustrative, not exhaustive. The key point is that to provide all of these and other benefits, access to data is essential. Laws restricting that access make the provision of many valuable services, and the convenience and benefits they provide, untenable. In the words of Alabama Attorney General Bill Pryor, it is consumers who ultimately “pay the price in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace.”⁶

Opt-In

One of the most severe restrictions on information flows in Congress and state legislatures, is the adoption of laws prohibiting the use of information about an individual unless the individual “opts-in” to the use by expressing affirmative consent. These “opt-in” requirements replace the longstanding standard of privacy protection in the United States, “opt-out,” under which personal information about an individual may be freely used within defined legal limits so long as the individual does not expressly prohibit such use.

We don’t have much experience with opt-in in the United States, because we have historically avoided such significant restraints on information flows. But there is a growing body of research about the impact of opt-in, and I would like to summarize six of the emerging findings.

1. Consumer Control over How Personal Information is Used. “Opt-in” and “opt-out” both give consumers the final say about whether his or her information is used. Neither approach gives individuals greater or lesser rights than the other. As a result, there is little difference in the privacy protection provided by “opt-in” and “opt-out” systems: under either system, it is the customer alone who makes the final and binding determination about data use. Shifting from an “opt-out” system to an “opt-in” system does not increase privacy protection, but it does have other dramatic effects.

⁶Bill Pryor, Protecting Privacy: Some First Principles, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, DC, at 4.

2. Economic Cost. There is a stark difference between “opt-in” and “opt-out” in terms of cost. An “opt-out” system presumes that consumers do want the convenience, range of services, and lower costs that a free flow of personal information facilitates, and then allows people who are particularly concerned about privacy to block the use of their information. Put another way, the “opt-out” system sets the default rule to “free information flow” and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an “opt-in” system presumes that consumers do *not* want the benefits stemming from publicly available information, and thereby turns off the information flow, unless consumers explicitly grant permission to use the information about them.

In other words, an “opt-in” system sets the default rule to “no information flow,” thereby denying to the economy the very lifeblood on which it depends. Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must build the pipeline by contacting one customer at a time to gain their permission to use information. Under opt-out, those customers can take advantage of 24-hour company web sites and 800-numbers that provide a wide range of services to opt-out. Consequently, an “opt-in” system for giving consumers control over information usage is always more expensive than an “opt-out” system. Opt-in requires that every consumer be contacted to gain explicit permission. Under opt-out, contact only occurs for those consumers who wish to withhold permission. Opt-in is more costly precisely because it fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them.

3. Consumer Expectations. One irony of the move to “opt-in” systems is that they are contrary to consumer expectations and behavior. The opinion polls that demonstrate that many consumers are increasingly concerned about their privacy also show that those same consumers are happy to have their personal information used for appropriate purposes so long as they are given an opportunity to “opt-out.”⁷

4. Customer Burdens. By requiring an explicit statement of permission prior to use of personal information, an “opt-in” system necessarily requires businesses to make extra contacts with consumers to determine whether they wish to “opt-in.” Since businesses lack the personal information necessary to identify which consumers are likely to be interested, their reliance on mass mailings to promote new products will mean that many consumers who have no interest whatsoever will receive “junk mail.”

To illustrate the cost of setting a default rule that halts the free flow of information, consider the experience of U.S. West, one of the few U.S. companies to test an “opt-in” system. In obtaining permission to utilize information about its customer’s calling patterns (*e.g.*, volume of calls, time and duration of calls, etc.), the company found that an “opt-in” system was significantly more expensive to administer, costing almost \$30 per customer contacted. To gain

⁷See, e.g., Personalized Marketing and Privacy on the Net: What Consumers Want, A Privacy & American Business Consumer Privacy Survey Questionnaire (Development and Report by Dr. Alan F. Westin, Fieldwork and Data Preparation by Opinion Research Corporation) (Nov. 1999).

permission to use such information for marketing, U.S. West determined that it required an average of 4.8 calls to each customer household before they reached an adult who could grant consent. In one-third of households called, U.S. West *never reached the customer*, despite repeated attempts. Consequently, many U.S. West customers received *more calls* than in an “opt-out” system, and one-third of their customers were denied opportunities to receive information about valuable new products and services.⁸

An “opt-out” system allows individuals with privacy concerns to prohibit certain uses of their information, but it also permits people who are less concerned about the privacy of basic information, such as that used in most direct marketing, to learn about new services and products they might value. In an “opt-in” system, the privacy-sensitive group gets the same level of protection, but both they and those consumers less concerned about privacy lose many opportunities to take advantage of information-dependent services, whether instant credit, targeted marketing, unified frequent travel programs, or personal shoppers.

5. Reduced Competition. “Opt-in” systems harm markets in other ways as well. Robert E. Litan, Director of the Economic Studies Program and Vice President of The Brookings Institution, and a former Deputy Assistant Attorney General for the United States, has written that switching from an “opt-out” system to an “opt-in” system would “raise barriers to entry by smaller, and often more innovative, firms and organizations,” make it more difficult for “companies to authenticate customers and verify account balances, and thus frustrate the ability to counteract fraud,” raise prices for many products and services “because competition would be reduced while fraud-related and marketing costs” would be higher, and deny opportunities to “consumers who now receive unsolicited material by phone or mail and act on those solicitations.”⁹

6. Constitutionality. The use of “opt-in” requirements in situations where no clearly defined, significant harm is threatened may very well violate the First Amendment. The Supreme Court has struck down many ordinances that would require affirmative consent before receiving door-to-door solicitations,¹⁰ before receiving Communist literature,¹¹ even before receiving “patently offensive” cable programming.¹² The words of the Court in the 1943 case of *Martin v. Struthers*—involving a local ordinance that banned door-to-door solicitations without explicit (opt-in) householder consent—are particularly apt:

⁸Brief for Petitioner and Intervenors at 15-16, *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).

⁹Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, in Lucien Rapp and Fred H. Cate, *European and U.S. Perspectives on Information Privacy* (forthcoming).

¹⁰*Martin v. Struthers*, 319 U.S. 141 (1943).

¹¹*Lamont v. Postmaster General*, 381 U.S. 301 (1965).

¹²*Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727 (1996).

Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household, and not upon the determination of the community. In the instant case, the City of Struthers, Ohio, has attempted to make this decision for all its inhabitants.¹³

One of the most important corollaries of the First Amendment is that the government may never interfere with expression to protect privacy if it cannot demonstrate that the interference is necessary to prevent a specific, identified harm. This was the view of the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc. v. Federal Communications Commission*, which the Supreme Court in June 2000 declined to review, when it struck down the rules of the Federal Communications Commission requiring that telephone companies obtain explicit (opt-in) consent from their customers before using data about their customers' calling patterns to market products or services to them. The court wrote that the government must show that the information the law would protect as private would inflict "*specific and significant harm*" on individuals: "Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* [the test applicable to commercial speech] for it is not based on an identified harm."¹⁴

Even assuming that telecommunications customers value the privacy of [information about their use of the telephone], the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. *Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.*¹⁵

Recommendations

So, for both practical and constitutional reasons, opt-in should be viewed as an exceptional tool that because of its high cost and unintended consequences should be reserved for exceptional situations where the risk of those costs and consequences is justified.

This is the ironic lesson from Europe, where the 1995 EU data protection directive requires businesses and governments alike to obtain affirmative consent before collecting or

¹³319 U.S. at 141.

¹⁴*U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 120 S. Ct. 1240 (2000) (emphasis added).

¹⁵*Id.* (emphasis added).

using any personal information.¹⁶ Many observers wondered how the European economy would be impacted by such a broad application of the “opt-in” requirement when it took effect in 1998. But, to date, national data protection authorities have permitted data collectors and users to rely on “opt-out”—what the Europeans call “implied opt-in”—for all but the most sensitive data. “Opt-in” may be the law on the books throughout Europe, but “opt-out” is the reality.

This cautious, restricted, with only one exception, is how we have historically viewed opt-in in the United States. (That exception is the Shelby amendment to the Department of Transportation Appropriations Act in 1999,¹⁷ which eliminates federal highway funds for states that do not require affirmative “opt-in” consent from individuals before information about them contained in driver’s and motor vehicle records is used for marketing and survey purposes. This is an anomaly that resulted from political posturing by Senator Shelby, which offends U.S. constitutional principles on both privacy and states’ rights. In any event, Idaho has already complied with this federal mandate.)

This caution is especially justified today, in the face of rapid technological change and the tremendous expansion of federal privacy law. The extensive privacy provisions of the Gramm-Leach-Bliley Financial Services Modernization Act¹⁸ are in the process of being implemented by federal and state regulators. We already know that under that law approximately 40,000 financial institutions will be sending as many as 2.5 billion notices to their various customers by June 12, 2001. Estimates are that individual households will receive an average of 20-50 notices each. Printing and mailing costs alone will be in the 2-5 billion dollar range, if not more. One may reasonably doubt the wisdom of a single state requiring additional notice without first waiting to see the effect of Gramm-Leach-Bliley’s extensive new requirements.

Similarly, the Clinton Administration has issued extensive regulations under the Health Insurance Portability and Accountability Act, restricting the use of medical information. Just last month the Administration, in response to more than 52,000 comments on its proposed regulations, has promised to implement even tougher rules by year end. Again, regulation by a single state in the face of such dramatically escalating federal action seems ill-advised.

The significant change and increase in the level of privacy protection afforded by federal law, and the obvious limits (and disadvantages to Idaho citizens and businesses) of a single state seeking to regulate information flows in a global environment, not only argue for caution, but also heighten the importance of Idaho lawmakers answering the constitutionally required question: What is the “specific and significant harm” that additional legislation is necessary to prevent that is not already the subject of an existing law? I believe you will be hard-pressed to

¹⁶Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data art. 25(1) (Eur. O.J. 95/L281).

¹⁷Department of Transportation and Related Agencies Appropriations Act, 2000, § 350, 106 Pub. L. No. 69; 113 Stat. 986 (1999).

¹⁸Gramm-Leach-Bliley Financial Services Modernization Act (S. 900), 106 Pub. L. No. 102, 113 Stat. 1338, 1436-1450, title V (1999).

find such a harm that is not already the subject of Gram-Leach-Bliley, the pending Health Insurance Portability and Accountability Act rules, the Fair Credit Reporting Act, or other federal or state law.

This does not mean that there is no additional role for the Idaho legislature, administration, and courts in protecting citizen privacy. Enforce existing privacy laws vigorously. This is especially important for the state Attorney General, who is given significant enforcement authority under both federal and state laws and activities that compromise the privacy of Idaho citizens. Before asking for more authority, use what you have.

Make sure that the government of Idaho has its own house in order. Only the government has the power to compel disclosure of personal information and only the government operates free from market competition and consumer preferences. Make certain that you are collecting no more information than necessary from and about your citizens; that you employ consistent, prominent information policies through public agencies; and that you protect against unauthorized access to citizens' personal information by government employees and contractors.

Take the steps that only the government can take to protect citizens against identity theft. Make government-issued forms for identification harder to obtain. Make the promise of centralized reporting of identity thefts a reality. Make it easier to correct judicial and criminal records and to remove permanently from one individual's record references to acts committed by an identity thief. No one but you can do this.

Finally, work with your agencies, public schools and universities, and private industry to educate the public about privacy and the tools available to every citizen to protect his or her own privacy. Teach the public about the 800-numbers citizens can call to be removed from mailing lists and prescreened offer lists, how to use the technology already in Internet browsers to protect against unwanted profiling and data collection, and about the steps that individuals can (and must) take to protect their own privacy. (This is especially true in the case of identity theft. Many of us are our own worst enemies when it comes to preventing identity theft, because of the cavalier way in which we select and use account names and passwords, disclose personal information to strangers, and fail to protect our credit cards and checks. Yet only we as individuals can take these steps.) Nothing can substitute for good judgment in the management of our personal information and identification documents for its effectiveness in combating identity theft and protecting our privacy. Yet few of us will recognize the importance of that responsibility or have the knowledge to fulfill it without education.

If, at the end of your inquiry, you believe that government intervention in markets is necessary, make certain that the government's action *responds effectively to a "specific and significant" harm in the least costly and intrusive way possible*. And whatever you do should apply to you as government officials and candidates as well as to business.

These are not easy issues; there are no easy answers. I appreciate the thoughtful, deliberative approach you are taking, and I am grateful to have had the opportunity to be some small part of it.