

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Trade, and Consumer Protection

Hearing on
PRIVACY IN THE COMMERCIAL WORLD
March 1, 2001

Statement of Professor Fred H. Cate

Mr. Chairman:

My name is Fred Cate, and I am a professor of law and director of the Information Law and Commerce Institute at the Indiana University School of Law in Bloomington. For the past 12 years, I have researched, written, and taught about information laws issues generally, and privacy law issues specifically. I directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, served as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and currently am a visiting fellow, addressing privacy issues, at the American Enterprise Institute.

I appreciate the opportunity to testify today and, more importantly, I want to acknowledge you and the Members of the Subcommittee for holding such a broad hearing on the subject of "Privacy in the Commercial World." It is a rare pleasure to participate in a hearing that is not restricted to a particular bill or event, but rather inquires widely about the uses of personal information, the need for further legislation, and the potential impact of adopting new privacy laws. Such an open-minded approach in an area as complex and important as privacy is desperately needed, and I applaud your leadership in providing it.

I would like to take advantage of the presence of the other distinguished members on this panel, who I believe will address a number of the issues posed by privacy laws, and limit my testimony to three points: the critical roles that information plays in our economy and society; the extent to which privacy laws inevitably interfere with the benefits that consumers enjoy as a result of accessible personal information; and the ways in which requiring consumer "consent" exacerbates, rather than ameliorates, the harmful impact of many privacy laws on consumers.

1. The Information Infrastructure

Information is the lifeblood of our 21st century economy. In the words of the Federal Reserve Board: "[I]t is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."¹ These simple words reflect a profound transformation: Consumers are increasingly evaluated today according to more complete, objective, and reliable information about them than was ever before possible. As a result, consumers can now expect—and the law can meaningfully require—that they be treated as *individuals* and judged on their own records, not by their race, gender, who they know, or other subjective prejudices. This is the result of the information revolution:

Routine, comprehensive information collection has contributed to unprecedented prosperity, and allows more Americans than ever before to share in that prosperity, and to do so on a more equitable basis. Consider the following examples of benefits that this “information infrastructure” makes possible.

a. Expanding the Availability, Enhancing the Speed, and Lowering the Cost of Consumer Credit

The routine sharing of reliable, standardized personal information has greatly expanded the availability, increased the speed, and reduced the cost of consumer credit. So, for example, when a consumer applies for a mortgage, car loan, or instant credit, the lender makes its decisions about whether, how much, and on what terms to lend based on information collected from a wide variety of sources over time. The lender can have confidence in that information because it has been assembled routinely—not just for the purpose of one loan application—and presents a complete picture of the borrower’s financial situation—not just one moment in time or information from just a selective sample of the businesses with which the borrower deals. Because of that confidence, lenders provide more loans to a wider range of people than ever before. Between 1956 and 1998, the number of U.S. households with mortgage loans more than trebled. The same trend is true for credit card products; today, the average American adult carries 13 credit cards.

Consumers benefit by obtaining the funds they need to buy homes and cars and finance educations. The “almost universal reporting” of personal credit histories, in the words of economist Walter Kitchenman, is the “foundation” of consumer credit in the United States and a “secret ingredient of the U.S. economy’s resilience.”² In addition, because the necessary information does not have to be collected from scratch, loan applications are reviewed and approved faster than ever before. In 1997, 82% of automobile loan applicants received a decision within an hour; 48% of applicants received a decision within 30 minutes.³ Many retailers open new charge accounts for customers at the point of sale in less than two minutes. This is unheard of in countries where restrictive laws prevent credit bureaus and other businesses from routinely collecting the information on consumer activities required to maintain the accurate, up-to-date files necessary to support rapid and accurate decision making.

The greater accuracy, speed, and efficiency of the credit system, and the greater confidence of lenders also drives down the cost of credit. Lenders don’t have to charge higher interest rates and fees to guard against bad or missing information. And it is easier for lenders to pool loans according to risk and sell them in the secondary market—a process known as “securitization.” This makes more capital available for new loans and further reduces the cost of credit in the United States by an estimated \$80 billion per year for mortgages alone.⁴ Most importantly, consumers benefit from the knowledge that loan decisions will now be based on their own financial situation, not on local biases or prejudices. Readily available, standardized personal information not only makes this possible, it also facilitates easy analysis of lender compliance with fair lending laws.

b. Identifying and Meeting Consumer Needs

Businesses use personal information to identify and meet customer needs. According to Federal Reserve Board Governor Edward Gramlich: “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.”⁵ In short, information-sharing allows businesses to ascertain customer needs accurately and meet those needs rapidly and efficiently. Detailed consumer information is at the heart of new individualized offerings that provide each customer with the recognition and personalized service that she desires.

c. Enhancing Customer Convenience and Service

Information-sharing also enhances customer convenience and service. For example, many services are provided through a myriad of companies. A customer may have a checking account, a savings account, a credit card, and an investment account all with the same bank, but the four services will likely be provided by four completely separate affiliates. The customer’s checks will be printed by a separate company altogether. Billing for the credit card may be handled by still another company. Because of information-sharing, the customer can deal with all six entities as if they were one. Her high savings balance may be used to qualify her for free checking. Overdrafts on her checking account can be covered automatically with her credit card. She can call one customer service number with questions, and if her credit card or checks are stolen, a single call is all that is needed to protect all of her accounts.

Many retailers provide specialty services and products, such as fine jewelry, photographic studios, vision services, hair care, and product repair or installation through independent companies that license the retailer’s name, but are not the retailer’s affiliates. This approach is required because of the nature of the service, efficiencies that come with specialization, insurance factors, and federal and state tax and licensure laws. Due to routine information-sharing, 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.

d. Targeting Interested Consumers

Information-sharing also allows consumers to be informed rapidly and at low cost of those opportunities in which they are most likely to be interested. As a result, information on second mortgages and home improvement services can be targeted only to home owners. Information on automotive products and services are targeted only to car owners. The American Association of Retired People can target its offers only to older Americans, veteran’s organizations can appeal only to people who have served in the armed forces, and political campaigns can target their solicitations to registered members of their party.

In the absence of information-sharing, these organizations either (1) could not afford to communicate with potential customers or members, or (2) they must contact even more households—meaning more unsolicited mail, e-mail, and telephone calls—to find people interested in their offer. The first alternative would mean the death of many organizations. In fact, 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. The second alternative means that the public is peppered with more mail, e-mail, and telephone calls, a higher percentage of which will be of no interest to the recipient. This would truly be “junk mail,” because it would have been generated without regard for the recipient’s demonstrated interests. Targeting marketing to consumer interests lowers the volume, cost, and environmental impact of that marketing while increasing consumer satisfaction.

e. Promoting Competition and Innovation

Information-sharing is especially critical for new and smaller businesses, which lack extensive customer lists of their own or the resources to engage in mass marketing to reach consumers likely to be interested in their products or services. This may help explain why some large European national banks and industrial concerns supported new privacy laws there: By restricting the availability of information about their customers, privacy laws help to protect established businesses from competition from other countries or start-ups. Open access to third-party information and the responsible use of that information for targeted marketing is essential to level the playing field for new market entrants.

Similarly, businesses offering specialized products and services rely on accessible information to help them identify and reach those customers most likely to be interested in their offerings, wherever those customers are located. Many businesses in today’s markets never see their customers because transactions are conducted exclusively by telephone, Internet, or mail. These businesses are able to serve the needs of potential customers they have never met because of the free flowing information that allows them to identify who those likely customers are. In a global market, information-sharing is key to connecting far-flung customers and businesses.

f. Preventing and Detecting Fraud

Another 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 more than \$12 billion in annual losses.⁶ Treasury Department officials estimated that credit card fraud losses would be between \$2 billion and \$3 billion in 2000.⁷ The insurance industry paid \$24 billion—10% of all claims—in 1999 for fraudulent property and casualty claims.⁸ The GAO found that Medicare made improper payments of \$13.5 billion in fiscal year 1999 alone, and has estimated that health care fraud accounts for up to 10% of national health care spending each year.⁹ Across the economy, business losses due to all forms of document fraud and counterfeiting exceed \$400 billion—6% of annual revenue of American businesses—per

year.¹⁰ Although businesses paid for virtually all of these losses, they 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. Close monitoring of account activity also allows credit providers, insurance companies, and other businesses to recognize unusual behavior that may indicate that someone is using a credit card or debit card without authorization or making improper claims. Moreover, because of information-sharing, companies share alerts about lost or stolen credit or debit cards and information about fraud schemes so that they can prevent further losses and improve the odds of apprehending the thief.

g. Informing the Electorate and Protecting the Public

Personal information is also used for a wide variety of purposes central to democratic self-governance and protecting public health and safety. For example, information is used to elect and monitor public officials and to facilitate public oversight of government employees and contractors. The Supreme Court has found that these uses are so critical that it has virtually eliminated any recourse by public officials or public figures for the publication of true information, even if defamatory or highly personal.¹¹

Law enforcement officials rely on collected personal information to prevent, detect, and solve crimes. Journalists and other researchers use accessible information to inform the public about matters of public importance. Personal information is also used for product safety warnings and recall notices, such as when Firestone and Ford Motor Company used databases to identify and obtain current addresses for people who own recalled Firestone tires.

Medical researchers rely heavily on personal information to conduct “chart reviews” and perform other research that is critical to evaluating medical treatments, detecting harmful drug interactions, uncovering dangerous side effects of medical treatments and products, and developing new therapies. Such research *cannot* be undertaken with wholly anonymous information, because the detailed data that researchers require will always include information that *could* be used to identify a specific person, and when that information indicates that a given therapy or drug poses a real health risk, researchers *must* notify the affected individuals.

Even information as mundane as citizen addresses is used to locate missing family members, owners of lost or stolen property, organ and tissue donors, and members of associations and religious groups and graduates of schools and colleges; and to identify and locate suspects, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. (This same information is used to help verify the identity of consumers who apply for instant credit, begin new utility service, or seek other valuable products and services.)

These examples are not exhaustive; they are mere illustrations of the extent to which personal information constitutes part of this nation's essential infrastructure, the benefits of which are so numerous and diverse that they impact virtually every facet of American life.

2. The Privacy Tension

All of the benefits outlined above flow from readily accessible information about consumers. To provide those and other benefits, access to data is essential. Laws and regulations designed to protect privacy interfere with that access and therefore with the benefits that result from open information flows. As a result, those laws—although motivated by the best of intentions—inevitably harm consumers. In the words of one state Attorney General, because privacy laws interfere with information flows, consumers ultimately pay the price for those laws “in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace.”¹² But the harm to consumers is also experienced through reduced convenience and service, an increased number of less well-targeted commercial solicitations, limited competition and innovation, and even diminished public health and safety.

3. The Limits of Consent

Proponents of new privacy laws often argue that these costs can be avoided because most privacy laws do not block information flows outright, but rather condition them on consumer *consent*. This reflects the recent dominant trend in privacy legislation—to invest consumers with near absolute *control over information*, what Alan Westin, in his path-breaking study *Privacy and Freedom*, described as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”¹³ The National Association of Attorneys General's December 2000 draft statement on Privacy Principles and Background sets forth as its core principle: “Put simply, consumers should have the right to know and *control* what data is being collected about them and how it is being used, whether it is offline or online.”¹⁴ And virtually all of the privacy bills pending before Congress reflect this goal: “To strengthen *control* by consumers” and “to provide greater individual *control*.”¹⁵

As a result, proponents of privacy laws argue that the costs of these laws can be avoided, because if consumers are persuaded that they benefit from information flows, they will consent to the collection and use of information about them. The simple, straightforward nature of this argument has made it very powerful. However, in addition to conflicting with Supreme Court precedent on the ownership of information¹⁶ and the protection of expression,¹⁷ this approach ignores the practical difficulty and burden to consumers of attempting to exercise control over the vast amount of data that they generate and disclose about themselves in an increasingly networked economy, and ignores the many powerful reasons why society permits access to information about others.

a. Unanticipated Benefits

The benefits of personal information are often unanticipated. For example, many retailers collect information about consumer purchases and then access that information so that consumers can return merchandise without a receipt, order supplies and replacement parts without knowing the exact model number or specific product information, obtain information about past purchases for insurance claims when fire or other disasters destroy or damage those goods, and receive immediate notification about product recalls and other safety issues. These are tangible benefits that many consumers take advantage of every day, but few consumers would anticipate in advance that they were going to need information about a past transaction for insurance purposes or to order replacement parts. The benefit is exceptionally valuable when it is needed, but often illusory before that time.

b. Lack of Consumer Contact

Many benefits result from uses of personal information that do not involve the consumer directly. For example, credit bureaus update consumer credit files—the files that are used to obtain rapid, low cost access to credit of all forms—without ever dealing directly with the consumer. In fact, few Americans will ever deal directly with a credit bureau. To require the credit bureau to establish contact with the consumer every time it needed to collect or use information about him or her would be expensive and burdensome to the consumer. Similarly, most mailing lists are obtained from third parties, not the people whose names are on the list. For a secondary user to have to contact every person individually to obtain consent to use the information would cause delay, require additional contacts with consumers, and increase costs.

c. Value of Standardized and Third-Party Information

There are many beneficial uses of personal information where the benefit, frankly, is derived from the fact that the consumer has *not* had control over the information. This is certainly true of credit information: Much of its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make not only that credit report useless, but all others, because lenders, merchants, employers, and others who rely on credit reports would not know which ones contained only selective information. Even when information is not particularly “positive” or “negative,” its value may depend on it being complete. Many businesses monitor accounts for suspicious activity that may indicate fraudulent activity. Often credit card companies will call a card holder whose account has experienced unusual charges to verify that the card has not been stolen. Identifying the *unusual* requires knowing what is *usual* and that, in turn, requires access to a complete set of data.

d. Consumer Preferences

Most consumers do not want to be deluged with repeated requests for consent. The ultimate result is that consumers will either not consent, and thereby diminish the benefits that flow from information-sharing both for themselves and others, or they will consent to everything, just to avoid further calls, letters, and e-mails. The *Los Angeles Times* reported in December 1999 that banking customers are understandably “irritated if the bank fails to inform them that they could save money by switching to a different type of checking account.” As the newspaper noted, however, “to reach such a conclusion, the bank must analyze the customer’s transactions.”¹⁸ One major U.S. bank reported that its customers who participated in a test of various privacy policies were annoyed at the very idea of being contacted by the bank to obtain permission to contact them again in the future to offer selected opportunities. Customers expected that the bank would use their information to offer them appropriate offers. The last thing they wanted was another phone call or letter asking permission to do what they perceived to be the very foundation of their relationship with the institution.

e. The Practical Obstacles to Consumer Contact

Conditioning use of personal information on specific consent may also harm consumers because of the practical difficulties of reaching them. Consider the experience of U.S. West, one of the few U.S. companies to test an “opt-in” system. To obtain 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 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, and one-third of their customers were denied opportunities to receive information about valuable new products and services.¹⁹

f. The Cost of Obtaining Consent

There is always a price to obtaining consent and recent experience has shown that those costs are often quite significant. For example, the privacy provisions of the Gramm-Leach-Bliley Financial Services Modernization Act require financial institutions to “clearly and conspicuously” provide customers with a notice about its policies and practices for disclosing personal information and informing customers about their right to “opt-out” of certain sharing of that information.²⁰ That disclosure must be made “[a]t the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship.”²¹ By July 1, 2001, approximately 40,000 financial institutions will be sending as many as 2-5 billion notices to their various customers. Households will receive an average of 20 or more notices each. Printing and mailing costs alone will run into the *billions* of dollars. Internal compliance costs are certain to be much higher.

“Opt-in” systems cost even more. The Department of Health and Human Services calculates that compliance with its recently released Health Insurance Portability and Accountability Act privacy rules will cost \$3.2 billion for the first year, and \$17.6 billion for the first ten years.²² Based on the prior, less complicated draft of the rules, health care consulting companies have calculated that the cost will be much higher—between \$25 and \$43 billion (or three to five times more than the industry spent on Y2K) for the first five years for compliance alone, not including impact on medical research and care or liability payments.

These costs are inevitably passed on to consumers. If the market will not bear the added cost, then these costs mean that the service or product will not be offered.

g. The Interconnectedness of Consent

Many of the beneficial uses of information that consumers now enjoy depend on spreading the cost of collecting and maintaining the information for a variety of uses. For example, commercial intermediaries collect, organize, and make accessible to the public government records. Those records are used for countless socially valuable purposes: monitoring government operations, locating missing children, preventing and detecting crime, apprehending wanted criminals, securing payments from “deadbeat” parents and spouses, and many others. In fact, in 1998 the FBI alone made more than 53,000 inquiries to commercial online databases for “public record information” that led to the arrest 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.²³ The Association for Children for Enforcement of Support uses information from public records, provided through commercial vendors, to locate over 75% of the parents they sought.²⁴ Access to these records is possible, as well as convenient and inexpensive, precisely because commercial intermediaries assemble the information for such a wide variety of other uses. If the law restricted the other valuable uses of public records, or made those uses prohibitively expensive, then the data and systems to access them would not be in place for *any* use. In as much as the beneficial uses of information outlined above are interconnected, and often depend on common systems and spreading the cost of acquiring and managing data over many uses, consent-based laws may only create the *illusion* of consent, because they will lead to consumers having fewer opportunities made available to them to which they *can* consent.

h. Required Consent

The opportunity for consent may also be illusory because many services or products cannot or will not be provided without personal information. HIPAA, for example, requires that physicians provide extensive disclosures and obtain explicit consent concerning information collection and use prior to treating a patient. If a patient wishes to be treated, she must consent. The law is effectively irrelevant, because the physician cannot treat the patient without information about his or her condition. Moreover, as a practical matter, signing the consent form is likely to become just another procedural hurdle, like signing an insurance authorization form, to

getting in to see a doctor. Experience suggests that few people will shop for physicians based on information policies; rather, their decisions about from whom to seek service will be driven by price, location, insurance coverage, specialty, and other considerations. So the expense of crafting, providing, and storing consent forms will likely achieve little in terms of enhancing consumer choice or privacy.

i. Consumer Ignorance and Lethargy

Finally, even if the request gets through to the intended adult recipient, the typical response to requests for consent to use personal information, to judge by the extensive experience of businesses and not-for-profit organizations, is that the customers will simply ignore them. Most unsolicited mail in this country is discarded without ever being read and most unsolicited commercial or fund-raising telephone calls are terminated by the consumer without the offer ever being made. It will not matter how great the potential benefit resulting from the information use, if the request is not read or heard, it cannot be acted on. Even where mail is actually read and the offer appeals to the consumer, lethargy and the competing demands of busy lives usually conspire to ensure that no action is taken. It is difficult to imagine that promises of potential future benefits from information use will command greater attention or activity.

These considerations suggest that simply conditioning the use of personal information on specific consent is tantamount to prohibiting outright many beneficial uses of information, because of the cost of obtaining consent, the extent to which consent may undermine information's usefulness, the degree to which uses of information are interconnected, and the many impediments to consumers receiving and acting on the request, even when it is in their best interest to do so.

Conclusion

The fact that information flows constitute a central part of our economic and social infrastructure, and that privacy laws—by interfering with those information flows—inevitably harm consumers and businesses, does not suggest that there is no role for the government or for law in protecting privacy. Far from it.

The government plays many critical roles in helping to protect individual privacy. One of the most important responsibilities of the government is assuring that its own house is 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. As a result, the government has special obligations to ensure that it complies with the laws applicable to it; collects no more information than necessary from and about its citizens; employs consistent, prominent information policies through public agencies; and protects against unauthorized access to citizens' personal information by government employees and contractors.

Similarly, there are many steps that only the government can take to protect citizens against privacy-related harms, such as 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. The government alone has this power.

Regulators and law enforcement officials should enforce existing privacy laws vigorously, and legislators should ensure that they have the resources to do so.

The government should also help educate the public about privacy and the tools available to every citizen to protect her own privacy. Many privacy protections can only be used by individuals—no one else can protect their privacy for them. Yet few individuals will recognize the importance of their responsibility or have the knowledge to fulfill it without education.

Finally, should you conclude that new laws or regulations are necessary, it is critical to identify and articulate clearly the purpose of the proposed privacy law or regulation, and whether it will in fact serve that purpose: In sum, what public benefit justifies the government's action? Only after having answered this question can the benefits of the proposed law or regulation be balanced against both the beneficial uses of information with which it interferes and the other costs of implementing and complying with the law. Armed with this information, you can then ask whether the law is worth its cost or whether there are other less intrusive, less expensive, or more effective tools for achieving the same purpose.

I address these and related issues in greater detail in a report that will forthcoming soon from the American Enterprise Institute. Because that document is so directly responsive to the subject of this hearing, with your permission, I append the complete draft report to my testimony.

Thank you again for the opportunity to testify.

Attachment

Biographical Statement

Fred H. Cate is a professor of law, Harry T. Ice Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington; senior counsel for information law with Ice Miller Legal & Business Advisors; and a visiting scholar at the American Enterprise Institute in Washington, DC.

He is a recognized authority on privacy and other information law issues. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities, was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and served as vice chair of the American Bar Association Section on Health Law's Electronic Communications and Privacy Interest Group. He currently directs the American Institute for Contemporary German Studies' project on Electronic Commerce in Europe and the United States.

Cate regularly appears before congressional and state legislative committees, and professional and industry groups on privacy and information law issues. He is the author of many articles and books concerning privacy and information law, including the award-winning *Privacy in the Information Age* and *The Internet and the First Amendment*. He writes widely for the popular press and has appeared on CNN, PBS, and many local television and radio programs. He received his J.D. and his A.B. with Honors and Distinction from Stanford University. A member of the boards of trustees of Phi Beta Kappa Fellows and of National History Day, he is listed in *Who's Who in American Law*.

He may be contacted at fcate@indiana.edu.

Notes

1. Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2* (1997).
2. Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns 1* (The Tower Group 1999).
3. Consumer Bankers Association, *1998 Automobile Finance Study* at 19.
4. Kitchenman, *supra*, at 7.
5. Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Banking and Financial Services, July 21, 1999 (statement of Edward M. Gramlich).
6. Barry Flynn, "In Search of Security, Some Banks Are Giving the Thumbs up to Fingerprinting New Customers," *Orlando Sentinel*, March 2000, at B1; Steven Marjanovic, "Banks Tap ATM Systems To Banish 18B Checks," *American Banker*, June 14, 2000, at 1.
7. Gary Fields, "Victims of Identity Theft Often Unaware They've Been Stung," *USA Today*, March 15, 2000, at 6A (quoting Undersecretary James Johnson of the U.S. Treasury Department).
8. "Insurance Fraud," *III Insurance Issues Update*, Oct. 2000.
9. General Accounting Office, *Medicare Improper Payments: While Enhancements Hold Promise for Measuring Potential Fraud and Abuse, Challenges Remain* (GAO/AIMD/OSI-00-281) at 4 (2000).
10. Association of Certified Fraud Examiners, *Report to the Nation on Occupational Fraud and Abuse* <<http://www.cfenet.com/newsandfacts/fraudfacts/reporttothenation/reportsection4.shtml>>.
11. *Monitor Patriot Co. v. Roy*, 401 U.S. 265 (1971).
12. Bill Pryor (R-Ala.), *Protecting Privacy: Some First Principles, Remarks at the American Council of Life Insurers Privacy Symposium*, July 11, 2000, Washington, DC, at 4.
13. Alan F. Westin, *Privacy and Freedom* 7 (1967).
14. National Association of Attorneys General, *Draft Statement on Privacy Principles and Background* at 7 (Dec. 11, 2000) (emphasis added).
15. S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong. § 2(b)(1) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001) (emphasis added)
16. See, e.g., *United States v. Miller*, 425 U.S. 435 (1976).
17. See, e.g., *Martin v. Struthers*, 319 U.S. 141 (1943); *Lamont v. Postmaster General*, 381 U.S. 301 (1965); *Denver Area Educational Telecommunications Consortium, Inc. v. Federal Communications Comm'n*, 518 U.S. 727 (1996).

18. Edmund Sanders, "Your Bank Wants to Know You," *Los Angeles Times*, Dec. 23, 1999, at A1.
19. Brief for Petitioner and Interveners at 15-16, *U.S. West, Inc. v. Federal Communications Comm'n*, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518).
20. Gramm-Leach-Bliley Financial Services Modernization Act tit.V, 106 Pub. L. No. 102, 113 Stat. 1338 (1999) (codified at various sections of 15 U.S.C.).
21. 15 U.S.C. § 503(a).
22. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (2000) (HHS, final rule) (to be codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).
23. Hearings before the Subcomm. for the Departments of Commerce, Justice, and State, the Judiciary and Related Agencies of the Senate Comm. on Appropriations, March 24, 1999 (statement of Louis J. Freeh).
24. Hearings before the House Committee on Banking and Financial Services, July 28, 1998 (statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis).