

PRESENTATION BEFORE THE TASK FORCE ON PRIVACY AND TECHNOLOGY

Tallahassee, Florida, August 25, 2000

Fred H. Cate¹

Mr. Chairman, ladies and gentlemen, it is a privilege to appear before Florida's Task Force on Privacy and Technology, and I thank you both for the opportunity to do so and for your warm hospitality.

Scope and Focus

"Privacy" has leapt to the top of the national political agenda. This issue has united the far right and far left, Republicans and Democrats, federal and state governments, the Eagle Forum and the ACLU, even Phyllis Schlafly and Ralph Nader. It has generated an avalanche of federal and state legislation, administrative regulations, hearings, litigation, press reports, and proposals for more to come in the future.

As a result, the first issue facing any state task force on privacy is what the scope and focus of the task force should be. I encourage you to focus on two related issues: (1) the protection of privacy in state and local governments' collection and use of information, and (2) the role of state and local governments in protecting citizens against identity theft. I recommend that you address these issues for six reasons:

1. Poll after poll tells us that no matter how concerned the public is about privacy in the private sector, we are more concerned about the *government* invading personal privacy. These concerns are well-founded, since only the government can compel disclosure of personal information and impose civil and criminal penalties for noncompliance, and only the government collects and uses personal information free from market competition and consumer preferences.
2. Government invasions of privacy have long been the focus of our constitutional privacy protections. There is no constitutional right to privacy in the private sector; only the government is constitutionally prohibited from unreasonably invading the privacy of citizens.
3. States have a limited role in the protection of privacy, especially in the context of information technologies. The Internet is inherently global; nations are currently wrestling with how national law can be effective in the online environment. It is hard to imagine that an individual state can, or should attempt to, regulate such a far-flung, rapidly changing medium. The issue is not merely state vs. federal regulation; it is

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.

also state vs. state regulation. It is presently impossible to determine with certainty the state from which an e-mail originates or in which a Web visitor resides. As a result, state regulation is impractical and, to the extent states adopt inconsistent regulations, impossible to comply with. The National Association of Attorneys General reached precisely that conclusion this summer when it decided against pursuing state privacy regulation in favor of supporting federal regulation.

4. Moreover, the federal government is rapidly shrinking the area in which states could regulate privacy in the private sector. Congress has passed comprehensive federal financial privacy legislation and is considering more. [□] The Clinton Administration has proposed sweeping health privacy rules which it has promised to implement before the end of the year. [□] The Federal Trade Commission has even reversed its longstanding opposition to federal privacy legislation applicable to the Internet and has sent not one but two proposals to Congress for such legislation in the past three months. [□] In short, the need for individual state action to protect privacy in the marketplace is rapidly diminishing.
5. I am mindful of your February deadline. Commissions and legislative committees have met for years without being able to agree on privacy standards for a single industry sector; with all due respect, I doubt whether this Task Force, no matter how well created or competently staffed, will be able to accomplish more in five months.
6. Finally, the important issues of how state and local governments facilitate citizens' privacy in your own collection and use of information, and how state and local governments can help stem the rising tide and reduce the cost of identity theft are well worth your time and uniquely within your control. The citizens of Florida deserve to have these issues addressed and you are the ideal—perhaps the only—body to be able to do so.

Principles for Protecting Privacy

Privacy advocates often talk of “fair information principles,” such as “notice” or “choice,” designed to protect consumer privacy. During the past 30 years, dozens of government, multinational, and private organizations has adopted a variety of such principles.⁵ While these

²Gramm-Leach-Bliley Financial Services Modernization Act (S. 900), 106 Pub. L. No. 102, 113 Stat. 1338, 1436-1450, title V (1999).

³Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (Nov. 3, 1999) (HHS, proposed rule).

⁴Federal Trade Commission, *Online Profiling: A Report to Congress (Part 2)—Recommendations* (July 2000); Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000).

⁵The first comprehensive set of these principles was articulated in 1973 by the U.S. Department of Health, Education and Welfare in *Records, Computers and the Rights of Citizens*. Since that time, additional versions of

sets of privacy principles overlap, they are most noteworthy for the extraordinary variety in both number and content of what each of these organizations considered to be the core principles necessary to safeguard privacy. I am not inherently opposed to such principles, I just don't know which set to use, or how they will apply in practice.

Instead of the “fair information principles” approach, I would like to offer seven observations—perhaps bordering on principles—that I believe should guide your thinking about information privacy issues and the role of the government in addressing them in any context—public or private. These are not as aspirational as “fair information principles,” but instead are based on constitutional law and the practical realities of U.S. society and markets.

1. Value of Open Information Flows

Citizens benefit from the open flow of personal information. As the Federal Reserve Board noted in its report to Congress on data protection in financial institutions, “it 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.”⁶ Those benefits are shared both by each consumer about whom data are shared and by all consumers in the aggregate because, as Federal Reserve Board Governor Edward Gramlich testified before Congress in July 1999, “[i]nformation 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.”⁷ Without reliable access to personal information, neither government nor business can anticipate and meet citizen and consumer needs, and service and convenience suffer as a result.

In 1998, Federal Reserve Board Chairman Alan Greenspan wrote to Congressman Edward J. Markey (D-Mass.): “A critical component of our ever more finely hewn competitive market system has been the plethora of information on the characteristics of customers both

privacy principles have been put forward in 1977 by the U.S. Privacy Protection Study Commission in *Personal Privacy in an Information Society*; in 1980 by the Organization for Economic Cooperation and Development in *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*; in 1995 by the Privacy Working Group of the Information Policy Committee of the U.S. Information Infrastructure Task Force in *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information*, the U.S. Department of Commerce in *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, and the European Union in Directive 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 (Eur. O.J. 95/L281); in 1996 by the Canadian Standards Association in *Model Code for the Protection of Personal Information: A National Standard of Canada*; and in 1998 and again this year by the U.S. Federal Trade Commission in *Privacy Online: A Report to Congress* (1998) and *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress* (2000).

⁶Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud 2* (1997).

⁷Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, U.S. House of Representatives, 106th Cong., 1st Sess. (July 21, 1999) (statement of Edward M. Gramlich).

businesses and individuals. . . . Detailed data obtained from consumers as they seek credit or make product choices help engender the whole set of sensitive price signals that are so essential to the functioning of an advanced information based economy such as ours.”⁸

The benefits that citizens enjoy from open information flows are especially clear in the case of public records. The personal information provided by the government serves critical functions in society:

- ▶ Journalists rely on the public record every day to gather information and inform the public about crimes, judicial decisions, legislative proposals, government fraud, waste, and abuse, and countless other issues.
- ▶ Law enforcement relies on public record information to prevent, detect, and solve crimes. In 1998 the FBI alone made more than 53,000 inquiries to commercial on-line databases to obtain a wide variety of “public source 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.”⁹
- ▶ Public record information is used to locate 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 public record information provided through commercial vendors helped locate over 75 percent of the “deadbeat parents” they sought.¹⁰
- ▶ Open public records help identify victims of fraud or environmental hazards; save lives by locating owners of recalled automobiles and blood, organ, and bone marrow donors; and protect consumers from unlicensed professionals and sham businesses.
- ▶ Researchers and journalists use public information for thousands of studies and articles each year concerning public health, traffic safety, environmental quality, crime, prisons, governance, and a vast array of other subjects.

⁸Letter from Alan Greenspan to Edward J. Markey, July 28, 1998 (available at <http://www.house.gov/markey/980728letter.htm>).

⁹Hearings 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).

¹⁰Hearings before the Committee on Banking and Financial Services, U.S. House of Representatives, 105th Cong., 2d Sess. (July 28, 1998) (statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis).

- ▶ Walter Kitchenman from The Tower Group has calculated that centralized, standardized, routinely gathered consumer credit information—assembled in large part from public records—makes it possible for U.S. lenders to provide mortgages and other loans more quickly and efficiently than anywhere else in the world, and at a cost-savings to U.S. consumers of \$80 billion a year.¹¹
- ▶ Check verification services use state motor vehicle records to help combat the 1.2 million worthless checks passed every day. One such service used that public record data to verify or warranty \$19 billion worth of consumer checks paid to more than 200,000 businesses last year, improving the speed and accuracy of check acceptances, fighting identity theft, and reducing check fraud.
- ▶ Cable companies and public utilities also use motor vehicle records to verify information about new customers, thereby helping people who have yet to develop credit histories establish new service.
- ▶ Our entire system of real property ownership and nearly all real estate transactions have long depended on public records. These records are used to confirm that the property exists, its location, and its defined boundaries. Buyers, lenders, title insurers, and others use these records to verify the title owner. Mortgages, many legal judgments, and other claims against real property cannot be collected without reference to public records.¹²

In a recent report on public record information, Richard Varn, Chief Information Officer of the State of Iowa, and I examined the critical roles played by public record information in our economy and society. We were struck by the extent to which such 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. . . .” The ready availability of public record data “facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want.”¹³

Restraints on information flows inevitably interfere with these and other benefits. This does not mean that those flows may never be restricted to protect privacy, but rather that before doing so, public officials should fully understand the value of the uses of personal information to be regulated and the impact of restricting them. In addition, public officials should be careful when distinguishing among uses of public records, because it is often one use that makes it economically viable for information to be available for another use. For example, the commercial public records databases that are used to detect and prevent fraud and locate fugitives and

¹¹Walter F. Kitchenman, *U.S. Credit Reporting: Perceived Benefits Outweigh Privacy Concerns* 7 (The Tower Group 1999).

¹²These and other examples are available in Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (1999).

¹³*Id.* at 10, 13.

missing children are not assembled for those purposes or paid for by those uses. Rather, it is independent, valuable commercial uses that make those databases and those additional uses possible.

2. Privacy Costs

Public officials should also be mindful of the cost of protecting privacy. Those costs take many forms. The cost of interfering with valuable information flows is discussed above. Two other types of costs warrant our attention. First, there are substantive costs to privacy. In a democracy and a market economy, privacy is not an unmitigated good: More is not necessarily better. Privacy facilitates the dissemination of false information, protects the withholding of relevant true information, and interferes with the collection, organization, and storage of information on which businesses and other can draw to make rapid, informed decisions.

This is well illustrated by the fact that virtually none of us want as much privacy for others as we do for ourselves. When we hire people to take care of our children, few of us are very interested in the caregivers' privacy rights. When we board an airplane, we don't want the pilots to have extensive privacy rights. The Supreme Court has long said that politicians have effectively no privacy rights. There are areas in which each of us intensely believes that we should have privacy rights, but few of us are seriously willing to accord those same privacy rights to others because of the costs that we perceive those rights as creating.

In addition to these substantive costs, however, there are also significant transactional costs. These costs are exacerbated by the fact that information is so fundamental to our economy and by the many different sources and often conflicting nature of privacy laws and regulation. The privacy provisions of the Gramm-Leach-Bliley Financial Services Modernization Act, whatever their advantages, are certain to prove hugely expensive to implement. 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. Yet one may reasonably wonder how much consumers will benefit from this onslaught of legal notices.

3. Constitutional Values

Every effort to protect privacy by interfering with information flows poses significant constitutional issues, especially under the First Amendment. When the government restricts information flows—for whatever purpose—it must do so as narrowly or, in some cases, in the least restrictive way possible. For example, when information is true and obtained lawfully, the Supreme Court repeatedly has held that the state may not restrict its publication without showing that the government's interest in doing so is "compelling" and that the restriction is no greater

than is necessary to achieve that interest.¹⁴ Under this standard, the Court has struck down laws restricting the publication of confidential government reports,¹⁵ and of the names of judges under investigation,¹⁶ juvenile suspects,¹⁷ and rape victims.¹⁸

Even if the information is considered to be “commercial,” its collection and use is nevertheless protected by the First Amendment. The Court has found that such expression, if about lawful activity and not misleading, is protected from government intrusion unless the government can demonstrate a “substantial” public interest, and that the intrusion “directly advances” that interest and is “narrowly tailored to achieve the desired objective.”¹⁹

In 1982 the Supreme Court struck down as unconstitutional a Massachusetts statute that required trial court judges to close all criminal trials when minor victims of sexual offenses testified.²⁰ It is difficult to imagine a stronger privacy interest than that of minor victims of sexual offenses who are having to testify at trial. But even in that instance the Supreme Court said the state may not enact an across-the-board rule closing trials. “In individual cases, and under appropriate circumstances, the First Amendment does not necessarily stand as a bar to the exclusion from the courtroom of the press and general public during the testimony of minor sex-offense victims. But a mandatory rule, requiring no particularized determinations in individual cases, is unconstitutional.”²¹ Laws that put in place broad restrictions on the flow of information, rather than requiring sensitive balances to prevent specified harms, are constitutionally problematic.

4. Focus on Reasonable Expectations of Privacy and Specific Harms

Among the most important constitutional values are the requirements that the law only protect reasonable expectations of privacy and only then if necessary to prevent specific harms. When evaluating wiretaps and other seizures of private information under the Fourth Amendment, the Supreme Court has long asked whether the data subject in fact expected that the information was private and whether that expectation was reasonable in the light of past experi-

¹⁴Florida Star v. B.J.F., 491 U.S. 524 (1989); Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979); Landmark Communications Inc. v. Virginia, 435 U.S. 829 (1978); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

¹⁵New York Times Co. v. United States, 403 U.S. 713 (1971).

¹⁶Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978).

¹⁷Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979).

¹⁸Florida Star v. B.J.F., 491 U.S. 524 (1989); Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

¹⁹Central Hudson Gas & Electric Corp. v. Public Service Comm’n, 447 U.S. 557, 566 (1980); Board of Trustees v. Fox, 492 U.S. 469, 480 (1989) (emphasis added).

²⁰Globe Newspaper Company v. Superior Court, 457 U.S. 596 (1982).

²¹Id. at 611 n.27.

ence and widely shared community values.²² There should be no interference with information flows to protect privacy interests that are not reasonable.

To be reasonable, courts have long held that *an expectation of privacy could not attach to public information*. No expectation of privacy may be reasonable if it involves information that is routinely and voluntarily disclosed or is available publicly. This reflects not only the Supreme Court's interpretation of the Fourth Amendment, but also the common sense that the law should not impose costly or burdensome impediments to the collection and use of information that consumers willingly disclose and that is widely available in the marketplace.

The law has also historically required that the government protect privacy interests *only when a specific harm is actually threatened*. 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 affirmative consent from their customers before using data about their customers' calling patterns to market products or services to them. The court wrote:

In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict *specific and significant harm* on individuals such as undue embarrassment or ridicule or intimidation or harassment or misappropriation of sensitive personal information for the purposes of assuming another's identity. 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.²³

This principle is justified not only by the need to avoid unnecessary restraints on valuable information flows, but also because it is only by identifying the harm that a law is designed to prevent or remedy that a legislator, reviewing court, or citizen can judge whether the law is necessary and whether it does, in fact, respond to that harm. The harm principle has largely been lost in the flood of proposed privacy legislation.

²²*Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *Terry v. Ohio*, 392 U.S. 1, 9 (1968); *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

²³*U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 120 S. Ct. 1240 (2000) (emphasis added).

5. Availability of Self-Help

Government intervention to protect privacy is in many ways ironic, because privacy protection in the United States has historically focused on *government* access to information. Government intervention to protect privacy is not only ironic, it is often counterproductive, because it often ignores and ultimately interferes with the considerable privacy protection available through the use of technologies, markets, industry self-regulation, competitive behavior, and individual judgment. Such nongovernmental protection is more flexible, more contextual, and better than that provided by broad laws, and that protection is achieved at potentially lower cost to consumers, businesses, and the society as a whole.

This is especially true in the context of the Internet, where readily available, easy-to-use technologies make meaningful privacy protection a reality. Laws and regulations designed to protect privacy may actually weaken it by ignoring, and even interfering with, the power of new technologies to protect privacy. For example, technological innovations such as adjustable privacy protection settings in both Netscape and Microsoft Explorer, encryption software, anonymous remailers, and in fact, the Internet itself all facilitate privacy and individual control over the information we disclose about ourselves. The widespread availability, increased power, and decreased price of many technologies also facilitates a vibrant market for privacy protecting software, devices, and services.

If privacy enactments make the Internet an inhospitable place for businesses to offer services and for consumers to shop, those opportunities for technological privacy protection will no longer exist. If the law creates a disincentive for developing privacy protection tools, then consumers will be left with less protection, not more. Remember, technologies can actually and completely protect privacy; law cannot. With more than half of all Web sites outside of the United States and therefore beyond the jurisdiction of our laws, and many more Web sites operated by individuals with little capital or reputations to risk, privacy law is simply less effective than technology at protecting privacy. To the extent we eliminate the incentive for the development of technological protections for privacy, not just online but in many other settings, we diminish the availability of real privacy for everyone.

6. Public Service Goal

The goal of all privacy law should be serving the interests of the public as citizens and consumers. Privacy is always in tension with other values—the benefits that come from the open flow of information, freedom from government intrusion in private markets and private lives, the prevention and detection of crime, consumer convenience, and countless other values that we seek and increasingly expect every day. If protecting privacy means that we no longer enjoy these and other benefits, the cost of privacy may simply be too great. And if the means we use to protect privacy are overly broad or intrusive, much of the cost of that protection will have been unnecessary.

The goal of all privacy law and regulation, therefore, should be achieving a balance between the value of open flow of information and the value of enhanced privacy protection to guarantee for consumers the maximum practicable benefit. To pass constitutional muster, as we have already seen, that balance must be as specific as possible. Such a balance is most likely to be reached if each consumer defines that balance for himself or herself. Consumers who value rapid convenient service more highly than absolute privacy should be free to make that choice. Therefore, privacy protection tools should give maximum control to individual consumers rather than require the government to decide an appropriate level of privacy protection for all. Maximizing consumer benefit, then, requires not only that privacy protection be balanced against the benefits that flow from accessible information, but also that the government avoid substituting its judgment for that of individual citizens.

7. Privacy Irrationality

Most people's privacy concerns are not logical. But this does not excuse the government from its obligation to adopt laws and regulations that are. The privacy arena has suffered from a spate of what can only be described as nonsensical laws. For example, many of these new privacy laws seek to protect information that is not private. The 1994 Drivers Privacy Protection Act restricts the disclosure of name and address information—the least private and most widely shared of all information—from motor vehicle records.²⁴ Moreover, the Act was enacted in response to the 1989 murder of actress Rebecca Schaeffer, who was stalked by an obsessed fan using information provided by a private investigator from her California Department of Motor Vehicles record. The law restricts the public's access to motor vehicle records, but not that of private investigators.

Moreover, many privacy laws, while imposing significant costs on consumers and businesses alike, fail to respond to any identified harm, much less one that is “specific and significant” as required by the First Amendment. For example, in an effort to protect privacy, California enacted a statute that prohibited the use of arrestee addresses obtained from law enforcement agencies for marketing products or services, but explicitly permitted such information to be used for “journalistic” purposes. It is difficult to take seriously the state's claim that sending a letter to an arrestee offering the services of an attorney or private investigator would invade her privacy, while publishing her name and address in the newspaper would not. This “overall irrationality,” as Justice Stevens called it in his dissent from the Supreme Court's decision upholding the constitutionality of the statute, “eviscerate[s] any rational basis for believing that the Amendment will truly protect the privacy of these persons.”²⁵

Florida was one of the states caught up in the controversy over the use of drivers license photos in a check-cashing database. It seemed like a great idea: Take advantage of the millions of already assembled digital photographs to provide a low-cost, easy-to-use product to help point

²⁴Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 18 U.S.C. §§ 2721-2725).

²⁵*Los Angeles Police Department v. United Reporting*, 120 S. Ct. 483, 492 (Stevens, J., dissenting).

of sale clerks verify the identify of a person wishing to cash a check. This would not only make it easier for consumers to write checks, especially out of state, but also help cut down on the \$12.6 billion lost to fraudulent checks every year. But the public, acting on little and often inaccurate information, was outraged, and public officials around the country responded with executive orders and laws prohibiting access to those records.

Pending efforts by legislators to prevent the use of Social Security Numbers and biometric identifiers—the key tools that private industry and law enforcement officials require to prevent and prosecute identity theft—in a misguided effort to protect privacy reflect a similar irrationality. Even laws that would seek to restrict access to basic public records in an effort to prevent their misuse, despite the fact that the information is widely available elsewhere and, at least in the case of identity theft, used by a friend or family member, are similarly ill conceived. Such laws are akin to closing off public highways to prevent theft: It is true that many thieves use public highways, but closing off the roads will not stop theft, but it will seriously burden the public and the economy. The understandable desire to “do something” in response to privacy concerns is all too often leading to nonsensical or counterproductive laws.

Identity Theft

This tendency toward irrational laws is particularly evident in the case of “identity theft.” Identity theft is often cited a critical impetus for new privacy laws. Unfortunately, because most of these laws restrict the private sector’s use of personal information, but not the government’s, they fail to address the most common tools for committing identity theft, while interfering with the responsible use of information that is necessary to provide consumers with the valuable products and services we want. Moreover, these laws often make it more difficult to prevent and detect identity theft, by making it harder to verify the identity of consumers. Privacy laws are seldom a remedy for identity theft, but rather a cause of it.

In reality, identity theft is a serious, complex, and rapidly growing problem that involves significant tensions between consumers’ desire for convenience, service, and privacy on the one hand, and protection from identity theft on the other. Preventing and detecting identity theft requires creative, thoughtful solutions—many of which involve the government.

Although identity theft is often thought of as a crime committed by strangers, this is often not the case. In one recent survey, 17 percent of the cases involved theft by someone the victim knew—a relative, friend, or business associate.²⁶ Some experts estimate that the real figures may be much higher. The Chief Credit Officer of Household International, Inc., testified before Congress in 1999 that half of all incidents of identity theft are committed by a *family member*.²⁷

²⁶CALPIRG and Privacy Rights Clearinghouse, *Nowhere to Turn: Victims Speak Out on Identity Theft 3* (2000).

²⁷Identity Theft, Hearings before the Subcomm. on Telecommunications, Trade & Consumer Protection and the Subcomm. on Finance and Hazardous Materials of the Committee on Commerce, U.S. House of Representa-

Robert Hartle, one of the most well-publicized victims of identity theft and now a leading victim's rights advocate, discovered that his personal information had been taken by the estranged husband of his mother.²⁸

Having obtained the personal information, identity thieves then use it to obtain identification documents (driver's licenses, birth certificates, Social Security cards, and passports); open charge accounts and lines of credit; take out mortgages and other loans; open bank accounts; write checks; purchase cars, airline tickets, and other goods; obtain telephone and utility service; run up long distance phone bills; and then, if caught, file bankruptcy—all in another person's name. Some perpetrators even use their false identities when stopped for speeding or arrested for other crimes. All of these activities are referred to collectively as "true name" fraud, because they involve engaging in fraudulent activities in the name of another real person.

The other common form of identity theft is "account takeover"—where a thief, rather than opening a new account or starting new service in someone else's name, instead takes over an existing account. This is usually done by changing the address on an account without the account-holder's knowledge or intercepting a renewal credit or debit card in the mail. The perpetrator then runs up the account to its limit, and may even change basic account information (such as address or password) to delay detection. According to one recent survey, two-thirds of identity theft cases involved "true name" fraud; 38 percent involved "account takeovers."²⁹

Apparently little identity theft today results from data disclosed on the Internet. According to one 2000 study of 66 victims of identity theft, only two believed that the thief had obtained their information via the Internet.³⁰ But the Internet both facilitates and is an hospitable environment for identity theft, so it seems sure to facilitate identity theft in the future.

Identity theft has many victims. The most obvious and most personally affected are the individuals whose identities are stolen. In one 2000 survey, individual victims estimated spending an average of 175 hours and \$808 (not including attorneys' fees) in out-of-pocket expenses to fix the problems caused by identity theft.³¹ In only 45 percent of the 66 cases examined did the victim consider the case to be solved; it took an average of 23 months to resolve those cases. The 55 percent who reported that their cases were still unresolved had been pending for an average of 44 months.³² Forty-nine percent used an attorney to help resolve their cases.³³ Attorneys' fees

tives, 106th Cong., 1st Sess., April 22, 1999 (statement of Charles A. Albright, Chief Credit Officer, Household International, Inc.).

²⁸Michael Higgins, *Identity Thieves*, *ABA Journal*, Oct. 1998.

²⁹*Nowhere to Turn*, *supra* at 4.

³⁰*Id.* at 5.

³¹*Id.* at 1.

³²*Id.* at 2.

³³*Id.* at 3.

ranged from \$800 to \$40,000.³⁴ In only 21 percent of cases was the thief arrested, often on unrelated charges.³⁵

“Even if they have no out-of-pocket costs,” Ada General Accounting Office has written, “individual victims can nonetheless suffer from injuries to their reputations and must undergo a sometimes very lengthy and agonizing process of clearing up their credit history. In the interim, these individuals may be unable to keep or find a job, obtain a home mortgage, or secure other time-critical loans, such as tuition loans for college-age children.”³⁶ Some victims are arrested for crimes they didn’t commit but that someone else, using their names, did commit. (In 15 percent of identity theft cases, the thief actually committed a crime and provided the victim’s information when he or she was arrested.³⁷) Other victims report being questioned when they re-enter the country from trips abroad because their passports are flagged to indicate pending warrants. Some victims are denied jobs or promotions because of bad credit, bankruptcy, or arrest records that are not their own. All victims report feeling violated; some are even tormented by calls and letters from the persons who stole their identities.

One harm that identity theft victims do *not* suffer is having to pay for the fraudulent charges that identity thieves rack up in their victims’ names. According to one survey, the total fraudulent charges involved ranged from \$250 to \$200,000 with an average of \$18,000.³⁸ Those charges are virtually always paid by the merchants from which the goods or services were fraudulently obtained, or the financial institutions who extended credit or whose charge or debit cards were fraudulently used by the identity thieves. These losses affect the businesses which must absorb them, as well as consumers through higher prices, inconvenience, and lost time and productivity.

The Role of the Government in Identity Theft

Until quite recently, many government agencies have done more to facilitate identity theft than to prevent or remedy it. For example, the government, motivated by a laudable desire to serve citizens, has made it easier than ever to obtain identification documents. Identity thieves take advantage of that new ease and use it to obtain fraudulent identification documents, such as drivers licenses and birth certificates. These, then, are the keys to unlocking an individual’s financial record.

Similarly, the government’s inability or unwillingness to correct judicial and law enforcement records has contributed significantly to the harm experienced by victims of identity

³⁴Id. at 4.

³⁵Id. at 3.

³⁶General Accounting Office, *Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited* 11 (1998).

³⁷*Nowhere to Turn*, *supra* at 3.

³⁸Id. at 2.

theft when they are arrested—often repeatedly—for crimes they did not commit, or they are denied benefits because of bankruptcies they did not file.

Virtually all victims of identity theft report that the injury they suffer is greatly exacerbated by the difficulty of working with the police and other government agencies to repair their credit and reputations, and apprehend the perpetrators. One identity theft victim, typical of the stories of many others, told the authors of a recent survey on identity theft: “The police department treated me as if I were the criminal.”³⁹ One victim reports being told by the police that “it was not their job.”⁴⁰ According to the authors of the survey, “[v]ictims reported the same difficulties with other government agencies they dealt with. Many responded that the Postal Inspector and the Department of Motor Vehicles told them nothing could be done, even if the theft had involved the victim’s mailbox or driver’s license.”⁴¹ This is the near-universal refrain from identity theft victims:

It is aggravating, debilitating and depressing beyond belief to meet with this kind of response at virtually every place one calls to get some assistance. One is advised to follow the proper channels, but the proper channels yield impotence at best, hostility toward the ‘annoying’ victim at worst. They are more like obstacles to tangible assistance.⁴²

Finally, both federal and state government bodies are considering bills restricting the use of the Social Security Numbers and biometric identifiers, such as fingerprints, in a misguided effort to protect privacy. These tools, far from invading privacy, are the key to accurately identifying citizens and reducing the prevalence of identity theft. One of the major issues concerning identity theft today is how to accurately separate data about one individual from data about another. This is made all the more difficult by the fact that approximately 16 percent of the U.S. population—about 42 million Americans—changes addresses every year; there are approximately 2.4 million marriages and 1.2 million divorces every year, often resulting not only in changed addresses, but also changed last names; and, as of 1998, there were 6 million vacation or second homes in the United States, many of which were used as temporary or second addresses.⁴³

The only reliable way to date to ensure that information about one consumer is not erroneously provided to another consumer or added to another consumer’s file is to organize those files by Social Security Number. Just a single segment of the modern economy—consumer

³⁹Id. at 6.

⁴⁰Id.

⁴¹Id. at 7.

⁴²Id.

⁴³Use and Misuse of Social Security Numbers, Hearings before the Subcomm. on Social Security of the Comm. on Ways and Means, U.S. House of Representatives, 106th Cong., 2d Sess., May 11, 2000 (statement of Stuart K. Pratt, Vice President, Government Relations, Associated Credit Bureaus, Inc.).

reporting agencies, *i.e.*, credit bureaus—processes 2 billion pieces of personal data on 180 million active consumers every month. Identifying those data by Social Security Number is the only reliable way of ensuring that they are attributed to the right person. Yet this is precisely what proponents of legislation designed to restrict the use of Social Security Numbers want to stop. They argue that such legislation is necessary to limit the availability of Social Security Numbers in the market and thereby reduce their availability for use in identity theft.

It is questionable whether legislation would have that effect, if every personnel record, every payment, and every interest-bearing or dividend-paying account still required a Social Security Number. It is therefore doubtful that restricting the use of Social Security Numbers by business will have an appreciable effect on diminishing their availability for identity theft. But it is certain that such a law would greatly increase the likelihood of identity theft and innocent errors by making it harder to identify specifically a unique individual. Government proposals to deny access to Social Security Numbers and other tools for authenticating identity turn the government into the unwitting accomplice of identity thieves.

Efforts to restrict the use of Social Security Numbers illustrate the irony that privacy protections, rather than being logically motivated by concerns about identity theft, are often wholly at odds with efforts to prevent identity theft. We must find better solutions.

Recommendations

I strongly encourage you to consider recommending to the Governor and the Legislature that Florida:

1. Collect no more information than necessary from and about its citizens. If you don't have it, you can't disclose it or use it in a way that harms citizens. Be the first state in the nation to publicly commit to scrutinize every way in which you collect data about your citizens to determine if it is really necessary. If you don't need the information, my advice to you is don't collect it.
2. Employ consistent, prominent information policies through Florida's public agencies. This does not mean that every privacy policy must be identical, but rather that citizens have a right to expect that the general principles that govern the collection and use of personal information will be consistent across agencies and technological media. I am not suggesting legal notices, but rather a clear, understandable statement of how and why you collect information about citizens, what you do with it, and what rights citizens have to access, correct, refuse to disclose, or restrict the use of data about them.
3. Enforce existing privacy and related laws. Florida already has significant protections for personal privacy and you only recently enacted increased penalties for identity theft. Enforce these laws vigorously before giving any consideration to adopting new laws.

4. Resist the urge to impose additional regulation on private industry's use of personal information—especially on the Internet—or to restrict access to Florida's historically open public records. Either course threatens the information infrastructure that is so essential to Florida residents and businesses. The risk of doing more harm than good is especially great in the face of sweeping new federal legislation, rapidly changing information technologies, and the limited time and resources you have to address such a sweeping, complex, and both constitutionally and economically significant subject.
5. Educate Floridians about privacy, the costs and benefits of protecting privacy, and the tools available to every citizen to protect his or her own privacy. Teach them about the 800-numbers they can call to be removed from mailing lists and prescreened offer lists, how to use the technology already in their Internet browsers to protect against unwanted profiling and data collection, and about the steps that they 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. *Nothing can substitute for good judgment in the management of our personal information and identification document for its effectiveness in combating identity theft and protecting our privacy.* Yet few of us will recognize the importance of that responsibility or the resources to help fulfill it unless the state helps educate us.

With specific regard to identity theft, I recommend the following essential steps:

1. Make government-issued forms for identification harder to obtain. Driver's licenses, state identification cards, birth certificates, and other forms of state-issued identification are the tools that the rest of the economy relies on to verify identity. If they are easily forged or fraudulently obtained or "taken over," then their value in the economy diminishes greatly, and the government actively disserves consumers and businesses alike. Today, a large percentage—perhaps a majority—of frauds committed by identity thieves involve obtaining new government-issued identification. The government must stop being the unwitting accomplice of identity thieves.
2. Make the promise of centralized reporting of identity thefts a reality. A single database should link all law enforcement agencies so that a victim can make a report to his or her local police department and have that information instantly be available to other law enforcement agencies across the country. Moreover, the government should establish a parallel or linked database to which anyone with a legitimate interest and appropriate consent of the individual involved can have access to verify that an incident of identity theft has been reported. This would create a first-in-the-national comprehensive "fraud alert" system that would help prevent any additional use of stolen identities, facilitate the identification of identity thieves, and provide victims of iden-

- tity theft with a single source to which they can direct creditors, employers, and others to verify claims of identity theft. This aids consumers directly, by helping them clear their names, but it also helps them indirectly, by allowing merchants to rapidly identify and assist consumers with legitimate identity theft claims, while also detecting the as many as 60 percent of claims that are erroneous or fraudulent.⁴⁴
3. 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 other than the government can perform this vital task, and the incidents of victims of identity theft being arrested—in some cases repeatedly—and denied jobs and other benefits because of crimes committed by others in their names illustrates the urgency of speedy action.
 4. Improve enforcement of identity theft and related crimes. Clearly, there have been significant improvements following passage of the Identity Theft Assumption and Deterrence Act, but enforcement requires financial and personnel resources that only the legislative branch can authorize. Moreover, effective enforcement often requires dedicated identity theft units. More innovative, well-funded approaches are necessary to put identity thieves behind bars and help victims clear their credit records and good names.
 5. Protect against unauthorized access to citizens' personal information by state employees and contractors. This is not merely a matter of having and enforcing policies against such access, but also of ensuring that employees and contractors are trained in basic precautions, such as not leaving terminals logged on when leaving the office, protecting passwords, and the like.
 6. Finally, avoid enacting laws that restrict the responsible availability and use of critical information that helps businesses authenticate the identities of consumers, manage information about them accurately and responsibly, and protect it from unauthorized access or use. Laws prohibiting the use of Social Security Numbers for identifying and separating consumer information, that limit the use of fingerprints and other biometric identifiers, or that restrict the ability of businesses and other organizations to verify the accuracy of consumer information with third parties greatly diminish the ability of businesses to protect consumers from identity theft. Similarly, the government should be careful to avoid imposing overly burdensome restraints on the responsible use of personal information that make beneficial services impossible, impractical, or unduly expensive. Preventing identity theft is a critical objective, but, as we have seen, many tools to achieve that end also interfere with providing the services

⁴⁴Alternative Dispute Resolution for Consumer Transactions in the Borderless Online Marketplace, U.S. Federal Trade Commission and Department of Commerce, June 6, 2000, at 148 (statement of Russell Schrader, Senior Vice President and Assistant General Counsel, Visa USA); Identity Theft, *supra* (statement of Charles A. Albright).

that consumers expect and demand. The government should be careful to balance any measure designed to protect against identity theft with the other costs it imposes on consumers and businesses.

Florida is known for many wonderful attributes, but perhaps none more important than its historical commitment to open government and open public records. As a professor of communications and media law, I can teach entire courses out of Florida cases and statutes alone, because of the extraordinary strides you have taken to make your government the most accessible and accountable in the nation. I urge you not to compromise that heritage, and I am confident that you do not need to do so to provide effective protection for Floridians' privacy and good names.

Again, I thank you for the opportunity to appear before you. I am happy to provide any assistance that I can as you carry out your important charge.