

Committee on Ways and Means
Subcommittee on Social Security
United States House of Representatives
Hearing on
ENHANCING SOCIAL SECURITY NUMBER PRIVACY
June 15, 2004

Prepared Statement of Professor Fred H. Cate

My name is Fred Cate, and I am a Distinguished Professor and director of the Center for Applied Cybersecurity Research at Indiana University, and a senior policy advisor at the Center for Information Policy Leadership at Hunton & Williams. For the past 15 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, was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and served as reporter for the recent Department of Defense Technology and Privacy Advisory Committee. A brief biographical statement is attached.

I appreciate the opportunity to testify today, and I am doing so on my own behalf. My views should not be attributed to Indiana University or to any other institution or person.

The Essential Role of Social Security Numbers

My research on information flows in both public and private sectors, and all of the other research in this field with which I am familiar, highlights the need for, and difficulty of, accurately identifying individuals and attributing information about them. At first glance, these may seem like straightforward activities, but they have proved exceptionally difficult. How do I know that the person presenting himself—to apply for instant credit, seek a government benefit, or board an aircraft—is who he claims to be? And how do I know that the data I have about him is correctly associated with the right person?

One example may suffice to suggest the magnitude of this challenge. The three national consumer reporting agencies process two billion pieces of personal data on 180 million active consumers every month to generate 600 million credit reports a year. Making certain that each of those two billion pieces of data is placed in the right one of 180 million files and that each file is provided only in connection with the individual it concerns is a daunting task.

The challenge is exacerbated by many factors, including:

- The frequency of common names (e.g., there are more than 60,000 John Smiths in the United States alone), and the fact that names are not constant, thanks in part to 2.3 million marriages and 1.1 million divorces every year.¹

¹ National Center for Health Statistics, *National Vital Statistics Reports*, vol. 51, no. 8, May 19, 2003, at 1, table A.

- The variety of addresses available to many people (e.g., home, office, vacation home, Post Office box), the fact that several people may share the same address, and the speed with which addresses and telephone numbers change: according to the U.S. Postal Service, approximately 17 percent of the U.S. population—about 43 million Americans—changes addresses every year; 2.6 million businesses file change-of-address forms every year.²
- The inconsistencies with which we record names (e.g., J. Smith, J.Q. Smith, John Q. Smith) and addresses (e.g., “123 Main,” “123 Main Street,” “123 Main St.,” “123 S. Main Street,” “123 Main Street, Apt. B”).
- The spread of first telephone and then Internet technologies, the increased mobility of the population, and the development of truly national competition mean that fewer transactions are conducted face-to-face, much less with people we know.

As a result of these and other factors, the need for a unique, ubiquitous, national, constant, and authoritative identifier has become inescapable. Many activities in which we engage in both public and private sectors are impossible or impractical without it. That is why the Social Security Number has evolved to fill this role: modern government and business activities required it to identify individuals, and ensure that information about one individual is not erroneously attributed to another individual. These two functions are often interrelated.

The identification function is often misunderstood. Obviously, the fact that an individual presents a Social Security Number does not prove that he or she *is* the person that the Social Security Number identifies. Rather, the Social Security Number provides an efficient, reliable way of locating a credit report or other record containing information that can then be used to verify the identity of a person. So, for example, if I apply for instant credit at a retailer, the retailer may ask for my Social Security Number as a way of locating a summary credit report about me. That credit report will list, among other things, my name, address, phone number, past addresses, and other identifying information. The retailer can then compare the information I have put on the instant credit application with the information contained in the credit report to determine if I am who I claim to be.

Two points are critical here: First, knowing my Social Security Number alone does not get me credit; it is merely a quick way of locating reliable information about me that then can be used to verify my identity. If you don’t believe me, walk in to any Target or Wal-mart or other retailer and try to obtain instant credit by presenting your Social Security Number alone.

The second critical point is that the underlying data store must be accurate and reliable. Social Security Numbers play an essential role here as well by helping to ensure that data are linked to the right individuals and that subsequent users of those data have confidence in the accuracy and completeness of the data. When you apply for instant credit or an auto loan or a mortgage the lender wants to know that it is seeing an accurate and complete picture of your

² United States Postal Service Department of Public Affairs and Communications, *Latest Facts Update*, June 24, 2002.

creditworthiness and that there will be reliable, affordable ways of determining if you declare bankruptcy or overextend yourself on credit in the future. Social Security Numbers facilitate the databases that do this.

Benefits of Ubiquitous Social Security Numbers

The availability and reliability of Social Security Numbers makes possible accurate and efficient national credit reporting and directly contributes to greater consumer choice, lower prices and interest rates, more widespread and affordable home ownership, and other benefits. Social Security Numbers facilitate commerce in other ways, for example, by making it easier to identify consumers remotely, thereby enhancing lender and seller confidence and reducing fraud.

The benefits of accessible Social Security Numbers are not limited to commerce. Social Security Numbers also play critical roles in identifying and locating missing family members, owners of lost or stolen property, heirs, pension beneficiaries, organ and tissue donors, suspects, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments. Just as with credit reporting, Social Security Numbers—often combined with other information, such as name—make it possible to construct accurate, comprehensive public record and third-party databases and search them quickly and reliably. Paula LeRoy from Pension Benefit Information testified before this subcommittee in 2001 that the presence of a Social Security Number increases the chance of locating a pension beneficiary from less than 8 percent to more than 85 percent—a greater than ten-fold increase.³ Moreover, Social Security Numbers can overcome inconsistencies in names or address or errors in the way this information is recorded.

Social Security Numbers are critical to identity verification and background checks required for airline employees, school bus drivers, child care workers, Defense Department and intelligence agency employees, and congressional staff. Post-September 11 programs for enhanced border, critical infrastructure, and passenger facility security all depend on being able to identify individuals and assess the risk they present by quickly connecting to accurate information about them. This is a substantial challenge, as stressed by the recent final report of the Department of Defense's Technology and Privacy Advisory Committee.⁴ Social Security Numbers are essential to this task.

The essential roles played by Social Security Numbers highlight the importance of today's hearing and of your longstanding efforts, Mr. Chairman, and those of this subcommittee to ensure the integrity and security of Social Security Numbers and to protect against their misuse. We must ensure that Social Security Numbers are accurate, unique, and available for responsible use. H.R. 2971 takes some important steps in this direction, for example, by getting Social Security Numbers off of identification cards and checks where they do not need to be displayed, and enhancing protections within the Social Security Administration for ensuring that

³ Hearing on Protecting Privacy and Preventing Misuse of Social Security Numbers before the Subcom. on Social Security of the House Comm. on Ways and Means, May 22, 2001 (statement of Paula Leroy).

⁴ U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 36-38 (2004).

Social Security Numbers are issued appropriately and securely. However, the breadth and importance of the roles played by Social Security Numbers raise concerns about some of the restrictions posed by H.R. 2971.

The Problem of Restricting Access Except for Specified Uses

H.R. 2971 would broadly restrict the “sale, purchase or display” of Social Security Numbers, subject to exceptions for certain uses—for example, credit reporting and national security. I applaud your attention to these critical needs. The problem, however, is that Social Security Numbers need to be associated with the underlying data from the start to ensure that they are included in appropriate databases and made part of the right files. So, for example, provisions authorizing the Attorney General to permit certain uses for national security purposes are important, but almost certain to be ineffective, because national security and law enforcement officials need—and regularly use—databases constructed for other purposes to access routine innocuous data to determine the risk that an individual may present. It is fine for the Attorney General to require that an individual entering a government facility or boarding an aircraft present a Social Security Number, but it will not matter at all if those numbers cannot be used to access properly segregated data in existing databases.

The FBI and other law enforcement agencies, for example, routinely access aggregate data collected and stored by Acxiom, ChoicePoint, LexisNexis, and other providers for many commercial uses. Allowing the FBI to use Social Security Numbers is important, but for the data to be reliable, the providers must have been permitted to use Social Security Numbers all along, and the government and private entities that supplied data to them must also have used them. Focusing only on the end user is inadequate.

The focus on use also ignores the fact that national security and law enforcement uses of Social Security Numbers frequently involve databases created for other purposes. Those other purposes subsidize the national security and law enforcement uses that the bill is likely to permit; if Social Security Numbers cannot be provided for those other purposes, they will not be available for the national security and law enforcement uses either.

The limitation of the display restriction to “the general public” is unlikely to ameliorate this risk, because of the breadth, vagueness, and circularity of the definition given the phrase “display to the general public”: “to make such number available in any other manner intended to provide access to the general public.” Moreover, as the General Accounting Office noted in its 1999 report to you, it is difficult to imagine that many data providers will undertake the cost and effort of maintaining two sets of data—one without Social Security Numbers for display to the general public and one without for other uses—or that data from which Social Security Numbers have been removed or obscured can be maintained, aggregated, and filed accurately.⁵ In addition, because violation of this provision is made a crime, subject to five years imprisonment, it seems likely that most businesses will steer clear of any activity that might be considered “display to the general public,” even if that means no longer providing valuable services that may very well continue to be legal.

⁵ General Accounting Office, *Social Security: Government and Commercial Use of the Social Security Number is Widespread* (GAO/HEHS-99-28) (1999).

The history of information flows is one of constantly evolving new and valuable uses. If those uses have to be approved one at a time through a legislative or regulatory process, they are less likely to evolve as quickly or to be as affordable when they do. Regulatory barriers might very well have restricted the unanticipated use of commercial records for locating parents delinquent with child support payments or retirees entitled to pension benefits. These uses were not anticipated when the databases on which they rely were first created, but they are valuable and important today.

Rulemaking Authority and Lack of Preemption

The many and vital benefits that the public enjoys as a result of ubiquitous Social Security Numbers are also threatened by the broad discretion given the Attorney General as to whether, and if so how, he might create exceptions to the bill's restrictions. As we have seen, any meaningful exception would likely result in undercutting significant portions of the bill. Narrower exceptions run the risk of not achieving the goals they are designed to serve and/or placing private- and public-sector custodians in the untenable position of maintaining duplicate databases or supplying data that may not be accurate or complete. The broad discretion given the Attorney General also creates a new regulator, parallel with the FTC which has long had authority in this area.

What is most surprising, however, in view of the need for a truly national identifier for national security, law enforcement, and commercial purposes is that the bill does not appear to expressly preempt state laws and regulations concerning the disclosure and use of Social Security Numbers. As Congress acknowledged last year with passage of the Fair and Accurate Credit Transactions Act, it is difficult to imagine anything more intrinsically national in scope than the creation of accurate, complete databases necessary to support national commerce, national security, nationwide law enforcement, and the fight against identity theft.

Incentives for Inaccuracy

Social Security Numbers are critical for maintaining data about individuals accurately. H.R. 2971, by restricting the use of Social Security Numbers, threatens to make databases less accurate. This is especially likely in the face of the proposed restriction on uses of credit header information, which is often the source of accurate, up-to-date data necessary to identify and locate individuals and which is already the subject of existing financial privacy law.

Nowhere is H.R. 2971's threat to accuracy more clear than in the provision prohibiting a person from doing business with an individual who will not provide a Social Security Number, unless federal law requires disclosure of the Social Security Number. The federal government has repeatedly acknowledged that it cannot maintain accurate records without access to Social Security Numbers; that is why the government requires them in such a wide range of settings even where no question of Social Security benefits is involved. But under this provision, the law would refuse to acknowledge that businesses face the same need; a business cannot refuse to provide a product or service to an individual who refuses to disclose his Social Security Number, even if that number is necessary to provide the product or service. The net result is certain to be

data less able to be linked accurately with the individual it concerns—an ironic outcome at the same time as Congress has mandated the FTC and other regulators explore ways of improving accuracy in credit reports and other databases.

Social Security Numbers and Identity Theft

The motivation behind proposed new restrictions on the use and availability of Social Security Numbers is preventing identity theft. Identity theft is a growing scourge of modern life. It takes a toll not only on the economy and businesses, who bear the lion's share of economic loss associated with the crime, but also on individuals who struggle sometimes for years to correct false information—information wrongly placed—in their commercial or government records. It is certain that much more needs to be done to address the rising tide of identity theft; my research suggests that restricting Social Security Numbers in government and commercial records is not the right step.

While we do not know as much as we need to about identity theft, thanks to the efforts of FTC and others, one important fact we are learning is that much—perhaps most—identity theft is not committed by a stranger, but by a family member, friend, or co-worker. According to the FTC's Synovate study of identity theft, published in September 2003 and based on more than 4,000 interviews, of the one-quarter of identity theft cases in which the victim knew the identity the perpetrator, 35 percent involved a "family member or relative" and another 18 percent involved a friend or neighbor. Another 23 percent of cases involved someone who worked at a company or financial institution that held the victim's financial information.⁶ Taken together, 76 percent of cases in which the perpetrator did identify the thief did *not* involve access to third-party data (e.g., commercial or public records) that appears to be the target of H.R. 2971.

In the remaining 24 percent of cases that might be affected by H.R. 2971, the role played by Social Security Numbers in identity theft is apparently the same as that played in other settings—namely, to link an individual to a database file (most often a credit report). Given the many valuable uses of Social Security Numbers and the many ways in which those numbers are available, it would be far more efficient, as well as more broadly effective, to focus on ways for improving the identification of the person with his file, rather than attempting to restrict access to the Social Security Number in the first place. So, for example, the law might creative incentives for credit grantors to take additional steps to ensure that the person is who he claims to be. This would held deter not only the 24 percent of identity theft cases that involve a stranger, but the other 76 percent that involve a friend, family member, or employee of a business with whom the victim has a relationship.

While our knowledge about identity theft is still developing, we do know that accurate Social Security Number information, attached to all financial information, is critical to fighting identity theft and to remedying it when it does happen. Social Security Numbers—if unique and reliable—are critical to preventing the granting of credit in somebody else's name. They are critical to keeping bad data out of innocent people's files. They are critical to identifying identity

⁶ Federal Trade Commission, *Identity Theft Survey Report* at 28-29 (2003).

theft when it occurs and notifying victims. Yet H.R. 2971 seems intended and likely to diminish their availability.

The FTC study reports that businesses lost \$47.6 billion due to identity theft.⁷ We should certainly be hesitant before imposing restrictions on Social Security Numbers that could add to that cost, especially if we cannot identify clear specific benefits from those restrictions. In addition, countless hearings, interviews with identity theft victims, and studies have shown that the greatest burden most identity theft victims face is clearing their good names. We should be hesitant before doing anything that would make that already difficult process any harder.

Finally, I would just note there is some risk of getting caught in an unending cycle. The need for a ubiquitous, reliable, unique identifier is not going to go away. If legislation makes Social Security Numbers unavailable, government and industry will devise another system of numbers. If Social Security Numbers today play a significant role in identity theft—and I have not seen evidence that they do—what leads us to think that the identifying number of the next decade won't play that same role?

Conclusion

Ubiquitous Social Security Numbers help identify people and ensure that information is associated with the correct person. These two critical roles are essential to many valuable activities—from facilitating national competition to locating heirs and missing children to enhancing national security. Accessible Social Security Numbers are also critical to preventing, detecting, and remedying identity theft, yet they appear to play little if any role in contributing to most cases of identity theft. This subcommittee would be well advised to continue its careful study of these issues; to enlist the FTC, the Social Security Administration, and other appropriate agencies in carrying out the research identified in H.R. 2971; to enact those measures necessary to enhance the integrity of the systems by which Social Security Numbers are created and assigned; to strengthen criminal penalties against the deceptive or fraudulent use of Social Security Numbers; and to identify and adopt specific measures to help victims of identity theft reclaim their good names easily and quickly. But I would urge the greatest caution before proceeding with any restrictions on the productive and value uses of Social Security Numbers necessary to the benefits consumers enjoy today, our economic resiliency, the prevention and detection of crime, and our national security.

⁷ Id. at 7, table 2.

Biographical Information

Fred H. Cate is a Distinguished Professor at the Indiana University School of Law—Bloomington and director of the Indiana University Center for Applied Cybersecurity Research. He specializes in privacy, security, and other information law issues.

Professor Cate served as reporter for the Department of Defense Technology and Privacy Advisory Committee, was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, and chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities. He is currently a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams and a member of Microsoft's Trustworthy Computing Academic Advisory Board.

He is the author of many articles and books, including *Privacy in the Information Age*, *Privacy in Perspective*, and *The Internet and the First Amendment*, and he serves on the board of editors of *Privacy & Information Law Report*. A senator and fellow of the Phi Beta Kappa Society and, Professor Cate received his J.D. and his A.B. with Honors and Distinction from Stanford University. He is an elected member of the American Law Institute and is listed in *Who's Who in America* and *Who's Who in American Law*.

Professor Cate may be contacted at:

Professor Fred H. Cate
Indiana University
School of Law—Bloomington
211 S. Indiana Avenue
Bloomington, IN 47405
Tel 812 855-1161
Fax 812 855-0555
fcate@indiana.edu