

**PREPARED TESTIMONY AND STATEMENT FOR THE RECORD
OF**

**DANIEL J. SOLOVE
ASSOCIATE PROFESSOR OF LAW
GEORGE WASHINGTON UNIVERSITY LAW SCHOOL**

HEARING ON

**“SECURING CONSUMERS’ DATA:
OPTIONS FOLLOWING SECURITY BREACHES”**

BEFORE THE

**SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION
COMMITTEE ON ENERGY & COMMERCE
U.S. HOUSE OF REPRESENTATIVES**

**May 11, 2005
2123 Rayburn House Office Building
Washington, DC**

I. INTRODUCTION

Mr. Chairman, members of the Committee, thank you for inviting me to appear before you and provide testimony. My name is Daniel Solove and I am an associate professor of law at the George Washington University Law School. I write extensively about information privacy law issues and have published well over a dozen law review articles as well as two books, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* (NYU Press December 2004) and *INFORMATION PRIVACY LAW* (Aspen 2003) (with Marc Rotenberg).

The announcement of recent data breaches at a variety of companies and institutions have affected millions of people. As one article notes:

In breaches reported publicly since February, more than 2.5 million records may have been exposed to thieves at data broker ChoicePoint, retailer DSW, news and information broker LexisNexis, the University of California at Berkeley and elsewhere.¹

I will not discuss the series of data breaches that have lead to this hearing, as I am sure that you are all familiar with them. Instead, I will focus my comments on what can be done to address the problems and how we can better protect information privacy. My remarks will focus on two points.

First, I will explain why the problem is larger than just a security problem. Security is one dimension of a larger set of issues involving information privacy. Beyond securing data, the law must ensure that when there is a leak or improper access, the harmful effects are minimized. Doing this requires empowering individuals with tools to better manage their data. Moreover, making companies more accountable for their activities will promote better security, as well as better accuracy, in record systems.

Second, I will discuss why the innovative role of the states should be preserved. Federal legislation must allow room for states to experiment with new approaches and solutions to the problem. Many current federal protections, as well as many of the ideas currently proposed to address the problem, are drawn from state laws.

There are many more specific measures that can be taken to address the problems we are encountering today. Chris Hoofnagle of the Electronic Privacy Information Center and I have written a short essay called *A Model Regime of Privacy Protection*, where we set forward succinctly a series of sixteen legislative proposals. We explain why these proposals are necessary and respond directly to the criticisms of our proposals by a wide array of individuals (some from the industries we propose regulating). The paper is currently available for free at:

Daniel J. Solove & Christopher Hoofnagle, *A Model Regime of Privacy Protection*
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701

I will avoid repeating the content of this paper, but I recommend that you read it as it may be helpful in crafting specific legislative solutions.

¹ Jon Swartz, *Time Warner's Personal Data on 600,000 Missing*, USA Today (May 3, 2005).

II. BEYOND SECURITY: A PROBLEM OF MANY DIMENSIONS

The litany of data leaks and improper access to personal data are the symptoms of a significant problem that Congress should address. It is important to understand the nature of the problem, as it extends far beyond just a security issue. In my recent book, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* (NYU Press, December 2004), I observed that the central problem we face is caused by a lack of individual participation and empowerment when it comes to the collection and use of personal information as well as a lack of accountability among the companies that handle the data. In my book, I argued:

We are increasingly living with digital dossiers about our lives, and these dossiers are not controlled by us but by various entities, such as private-sector companies and the government. These dossiers play a profound role in our existence in modern society.²

These repositories of personal information are used in ways that affect key aspects of our lives: whether we get a loan, a license, or a job. However, despite these high stakes:

At present, the collectors and users of our data are often not accountable to us. A company can collect a person’s data without ever contacting that person, without that person ever finding out about it. The relationship is akin to the relationship between strangers—with one very important difference: One of the strangers knows a lot about the other and often has the power to use this information to affect the other’s life.³

The problem is not that companies dealing with personal information are a bunch of evil-doers bent on harming people. The collection and use of personal information can have many benefits, and the goal of an effective protection of privacy is not to stop information flow, but to empower individuals with greater control over their data and to make companies more accountable for their uses of personal data.

A. Individual Participation

People lack much participation in how their data is used or disseminated. Personal data is readily collected and disseminated without people’s knowledge and consent, thus increasing people’s vulnerability to identity theft, stalking, and other crimes.

Identity theft is rising at an staggering rate. In an identity theft, the thief uses a victim’s personal information to improperly access accounts, obtain credit in the victim’s name, or impersonate the victim for other purposes. In 2003, the FTC estimated that “almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the past year.”⁴

² DANIEL J. SOLOVE, *THE DIGITAL PERSON; TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 115 (2004).

³ *Id.* at 102.

⁴ FEDERAL TRADE COMMISSION, *IDENTITY THEFT SURVEY REPORT* 4, 6 (Sept. 2003). For an excellent account of the rise of identity theft, see BOB SULLIVAN, *YOUR EVIL TWIN: BEHIND THE IDENTITY THEFT EPIDEMIC* (2004).

The law has attempted to deal with identity theft by enhancing criminal penalties, but this alone has been a dismal failure. The problem is that identity thieves are hard to catch. Gartner, Inc. estimates that only 1 in 700 thieves is successfully prosecuted.⁵ A report by the U.S. General Accounting Office describes in great detail the difficulties with criminal investigation and prosecution of identity theft cases.⁶

In contrast, I noted in my book that:

The identity thief’s ability to so easily access and use our personal data stems from an architecture that does not provide adequate security to our personal information and that does not afford us with a sufficient degree of participation in its collection, dissemination, and use. Consequently, it is difficult for the victim to figure out what is going on and how to remedy the situation.⁷

The problem is that the law does not afford people sufficient participation in the way that their information is managed. Identity theft is difficult for victims to detect because they have little knowledge about the information being circulated about them or how that data is being used. The victim’s lack of awareness is exploited by the identity thief, who can go on a spree of fraud in the victim’s name without the victim finding out about it. Therefore, solutions to the problem must provide individuals with greater knowledge and control about how their data is used.

B. Remedies for Harmed Individuals

People must be provided meaningful remedies when their data is leaked or misused. Without meaningful remedies, mere notice of a leak would be akin to a company saying: “We just had a toxic spill in your backyard. It might cause you harm, and so you might want to have periodic medical checkups.” The letter from ChoicePoint to the victims of its data breach began:

I’m writing to inform you of a recent crime committed against ChoicePoint that MAY have resulted in your name, address, and Social Security number being viewed by businesses that are not allowed to access such information. We have reason to believe that your personal information may have been obtained by unauthorized third parties, and we deeply regret any inconvenience this event may cause you.⁸

The letter recommended that people review their credit reports, and continue to check them for unusual activity. In other words, “we’ve had a spill, now you go and protect yourself.”

Certainly, requiring disclosure of security leaks is a good first step, but merely sending people a scary letter without providing them with sufficient rights and abilities to address the problems will not suffice.

⁵ Stephen Mihm, *Dumpster Diving for Your Identity*, N.Y. Times Magazine, Dec. 21, 2003.

⁶ U.S. General Accounting Office, Report to the Honorable Sam Johnson, House of Representatives, Identity Theft: Greater Awareness and Use of Existing Data Are Needed 17-18 (June 2002).

⁷ DANIEL J. SOLOVE, *THE DIGITAL PERSON; TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 115 (2004).

⁸ Letter from ChoicePoint to Californians Regarding the Data Breach (Feb. 9, 2005).

Identity theft, according to estimates, results in victims spending on average 200 hours and thousands of dollars fixing the damage.⁹ Becoming victimized by identity theft is akin to contracting a chronic protracted disease. Because people have so little participation and power over their information, it is very hard for them to cure themselves and clean up their records. Identity theft can be financially and emotionally crippling, and the law does little to help people who have been victimized. States, such as California, have adopted some effective measures to assist victims in dealing with identity theft.¹⁰ I believe that Congress should look to California’s measures as it crafts a federal law addressing these issues.

C. Deactivating Dangerous Data

The data leaks that have occurred recently are made more harmful because of another type of security issue. SSNs, birth dates, and other pieces of personal data are used by other companies as passwords to obtain access to accounts or to sign up for a credit card. It would take great imagination to design a poorer security mechanism than the use of SSNs. This is akin to using a password that anyone can readily obtain in an instant. Companies routinely sell people’s SSNs, as it is not illegal to do so. SSNs are also available in many public records.¹¹ This “password” can then unlock virtually any account or be used to sign up for credit cards. And it is very difficult to change it. As I argued in my book “the SSN functions as a magic key that can unlock vast stores of records as well as financial accounts, making it the identity thief’s best tool. . . . [T]he government has created an identification number without affording adequate precautions against its misuse.”¹²

If the practice of using SSNs as passwords were halted, the leakage of SSNs would not be as dangerous and damaging to individuals. In our paper, *A Model Regime of Privacy Protection*, Chris Hoofnagle and I propose:

Companies shall develop methods of identification which (1) are not based on publicly available personal information or data that can readily be purchased from a data broker; and (2) can be easily changed if they fall into the wrong hands. Whereas Social Security Numbers cannot be changed without significant hassle, and dates of birth and mother’s maiden names cannot be changed, identifiers such as passwords can be changed with ease. Furthermore, they are not universal, and thus a thief with a password cannot access all of a victim’s accounts – only those with that password. Biometric identifiers present problems because they are impossible to change, and if they fall into the wrong hands could prove devastating for victims as well as present ongoing risks to national security. Therefore, passwords are a cheap and effective way to limit much identity theft and minimize the problems victims face in clearing up the damage caused by identity theft.¹³

⁹ Janine Benner, Beth Givens, & Ed Mierzewski, *Nowhere To Turn: Victims Speak Out on Identity Theft: A CALPRIG/Privacy Rights Clearinghouse Report* (May 2000), at <http://privacyrights.org/ar/idtheft2000.htm>.

¹⁰ The California Office of Privacy Protection maintains a comprehensive summary of California’s privacy statutes: <http://www.privacy.ca.gov/lawenforcement/laws.htm>.

¹¹ SOLOVE, DIGITAL PERSON, *supra*, at 115-17.

¹² SOLOVE, DIGITAL PERSON, *supra*, at 116.

¹³ Daniel J. Solove & Christopher Hoofnagle, *A Model Regime of Privacy Protection*, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=699701

If businesses and other private sector organization were restricted from using SSNs as passwords, improper access to people’s SSNs would not put people in such peril of identity theft and fraud.

The Gramm-Leach-Bliley (GLB) Act of 1999 requires agencies that regulate financial institutions to promulgate “administrative, technical, and physical safeguards for personal information.”¹⁴ Despite the fact that FTC regulations under the Gramm-Leach-Bliley Act establish security standards for financial institutions to “[p]rotect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer,”¹⁵ many financial institutions continue to allow easy access to records by using SSNs as passwords. In an article entitled, *Identity Theft, Privacy, and the Architecture of Vulnerability*,¹⁶ I argued:

The GLB Act requires a number of agencies that regulate financial institutions to promulgate “administrative, technical, and physical safeguards for personal information.” On February 1, 2001, several agencies including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision issued standards for safeguarding customer information. On May 23, 2002, the FTC issued similar security standards. Pursuant to the FTC regulations, financial institutions “shall develop, implement, and maintain a comprehensive information security program” that is appropriate to the “size and complexity” of the institution, the “nature and scope” of the institution’s activities, and the “sensitivity of any customer information at issue.” An information security program consists of “the administrative, technical, or physical safeguards [institutions] use to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle customer information.” The regulations set forth three objectives that a security program should achieve:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The GLB Act is on the right track in its focus on information security. . . . However, the regulations under the GLB Act remain rather vague as to the specific level of security that is required or what types of measures should be taken. The regulations require institutions to designate personnel to “coordinate” the information security program; and to “[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.” These regulations establish rather broad obvious guidelines; they virtually ignore specifics. Of course, a rule that is too detailed in the standards it required could end up being ineffective as well. . . . [S]uch regulations, if too specific, can quickly become obsolete, discourage innovation, and be costly and inefficient. However, rules that are too open-ended and

¹⁴ 15 U.S.C. § 6801(b) (requiring agencies to promulgate “administrative, technical, and physical safeguards for personal information.”).

¹⁵ 16 C.F.R. § 314.3(b) (2002).

¹⁶ Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 *Hastings L.J.* 1227 (2003).

vague can end up being toothless. Although security standards must not be overly specific, they must contain meaningful minimum requirements.

Ultimately, the strength of the GLB Act’s security protections will depend upon how they are enforced. . . .

Despite these new security provisions, companies continue to maintain lax security procedures for the access of financial accounts and other personal data. Thus far, the FTC’s efforts have been somewhat anemic. With vigorous enforcement, security practices can change. But it remains uncertain whether the FTC and other agencies will undertake such a vigorous enforcement effort.¹⁷

The FTC has not used the GLB Act to crack down on security, as the spate of security breaches in the news these days have occurred in spite of these regulations. The FTC could have concluded, for example, that the use of SSNs as passwords by so many financial institutions was an insufficient security procedure under the GLB standards. But it did not. Why hasn’t the FTC vigorously enforced these security standards?

I can postulate two reasons. First, the security standards only apply to financial institutions rather than all the entities that process significant amounts of personal data. Second, they are rather vague, and as a result, they have not provided adequate guidance. To be effective, security standards must apply widely, not in a piecemeal fashion, and they must be more specific in nature (without being overly constraining).

D. Accuracy

Beyond identity theft, people lack the ability to easily locate and fix errors in their records that can cause them harm. Decisions are being made based on people’s dossiers which are often riddled with inaccuracies. Although a recent *Wall St. Journal* article noted that ChoicePoint says that only .0008% of its 7.3 million background checks in 2004 had incorrect data, the authors had no difficulty finding a number of instances of people harmed by errors in ChoicePoint databases.¹⁸ In one study, 90% of ChoicePoint’s reports obtained had at least one error.¹⁹ And there are numerous anecdotal stories reported in the media of significant errors in people’s reports.²⁰

The issue of accuracy demonstrates a central problem -- the companies maintaining personal data are often not accountable to the people to whom the data pertains. Because of this lack of accountability, there are insufficient incentives for data brokers to maintain their records accurately. The Fair Credit Reporting Act (FCRA) requires consumer reporting agencies to maintain procedures to ensure “maximum

¹⁷ *Id.* at 45-46. The article is available online at:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416740

¹⁸ Evan Perez & Rick Brooks, *File Sharing: For Big Vendor of Personal Data, A Theft Lays Bare the Downside*, *Wall St. J.*, May 3, 2005, at A1.

¹⁹ *After the Breach: How Secure and Accurate is Consumer Information Held by ChoicePoint and Other Data Aggregators?*, Before the California Senate Banking Committee, Mar. 30, 2005 (testimony of Pam Dixon, Executive Director, World Privacy Forum).

²⁰ *Id.* (testimony of Elizabeth Rosen, Registered Nurse) (noting that the report wrongly reported that she owned a deli store); Bob Sullivan, *ChoicePoint Files Found Riddled With Errors*, *MSNBC*, Mar 8, 2005, available at <http://www.msnbc.msn.com/id/7118767/> (noting that Deborah Pierce’s ChoicePoint report wrongly indicated a “possible Texas criminal history”).

possible accuracy.”²¹ However, many data brokers have databases that they claim fall outside of FCRA. And they gather data from various public record systems, which themselves might have errors. An error can infect various databases because of the fluidity by which personal information is transferred. Moreover, because people are so out of the loop when it comes to the way their data is collected and used, they might not even discover the error. Little is done more systemically to ensure the accuracy of record systems used for background checks and other decisions about people’s lives.

E. Closing the Gaps

The security breaches we are facing today are part of a larger problem, one involving information privacy. This is not a problem that can be solved with what I call the “little more care and little more notice” approach. Certainly setting minimum security standards and providing notice to consumers of security breaches are two important steps. But the larger problem is one of information privacy. In some contexts, personal information is widely collected, used, and disseminated without much control or limitation. Information today is protected in a piecemeal fashion based on who holds it. The same piece of data might be protected if held by a video rental store but completely unprotected in the hands of data brokers such as ChoicePoint or LexisNexis.²² The current state of regulation of information is very porous, with tremendous gaps and loopholes. The result is that we have, in many respects, lost control over the way personal information is collected, managed, and used. We have a system that does not promote accountability among the users of personal information. We have a system that to a large extent leaves people out in the cold if victimized by identity theft or if harmed by an erroneous report. We have a system that thrusts on consumers the tremendous responsibility of guarding their digital dossiers, a difficult task when so many companies maintain data about them and when people have little knowledge that this is going on. Congress must put individuals back in control of their data and ensure that companies are accountable for the way they handle and use that data.

III. THE PROBLEM WITH PREEMPTION

In any solution that Congress takes, the innovative role of the states must be preserved. Thus, Congress should avoid preempting state laws when crafting federal legislation.

Many of the ideas for reforming the information system in this country emerge from state laws. Justice Brandeis said it well: “It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.”²³ This is especially important in such a rapidly changing field such as information privacy. Not all approaches work, and we need a way to test innovative solutions. Indeed, the law that required ChoicePoint to disclose its security breach was a

²¹ 15 U.S.C. § 1681e(b).

²² Video Privacy Protection Act of 1998, Pub. L. No. 100-618, 18 U.S.C. §§ 2710-11.

²³ *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

California law. What if there were federal preemption and such a law never existed? Would we ever have found about the security breach?

Federal legislation that preempts state law will not only shut down the real engines of innovation in the field, but it will have very detrimental long-term effects on federal legislation as well. The grist for federal legislation in privacy is often state regulatory ideas that have worked. The majority of privacy legislation has been enacted at the state level.²⁴ Many of the federal laws addressing privacy have adopted measures tried-and-tested in the states. The states first tried out the idea of telemarketing do-not-call lists. Many of the reforms in the 2003 federal Fair and Accurate Credit Transactions Act were based on prior state laws.²⁵ If Congress were to shut down this tremendous source of ideas, federal legislation will lose one of its primary developmental tools. Federal legislation in the future would suffer severely as a result.

I have often heard companies say that it is too onerous complying with so many differing laws in all 50 states. Yet if the federal legislation sets a strong floor of protection, there will be little incentive for the states to do more. In other words, if the federal legislation solves the problems, then there will not be a need for the states to act. Additionally, historically, stronger protections have only been enacted by a handful of states, not all 50. So the reality is not 50 different standards, but a floor of protection for 90% of the states with the remaining 10% adopting a slightly more protective standards. Moreover, other industries have long dealt with differing state protections, such as the auto industry and the insurance industry. Why are the burdens on data brokers any greater? What strikes me as most remarkable is that companies that manage billions of records of data and claim to be able to do so with remarkable depth, precision, and detail say that they cannot comply with a handful of states that have stronger protections.

Most federal privacy laws have not preempted stronger state protections: the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Driver’s Privacy Protection Act, and the Gramm-Leach-Bliley Act.²⁶ In all these instances, companies have been able to comply with state laws.

IV. CONCLUSION

I am very encouraged that so many in Congress are interested in addressing the problems of data security and information privacy. My recommendations today are: (1) to focus on the larger problem by empowering individuals and making the users of data more accountable; and (2) to avoid preempting the states, as this will retard the development of privacy law for years to come.

²⁴ ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS (Privacy Journal 2002).

²⁵ Edmund Mierzwinski, *Preemption of State Consumer Laws: Federal Interference Is A Market Failure*, Government, Law and Policy Journal of the New York State Bar Association, Spring 2004 (Vol. 6, No. 1, pgs. 6-12).

²⁶ Respectively at 18 U.S.C. § 2510 et. seq., 12 U.S.C § 3401, 47 USC § 551(g), 18 USC § 2710(f), 29 USC § 2009, 47 USC § 227(e), 18 U.S.C. § 2721, and Pub. L. No. 106-102, §§ 507, 524 (1999).