No. 02-1377

IN THE

Supreme Court of the United States

BUCK DOE,

Petitioner,

v.

ELAINE L. CHAO, SECRETARY OF LABOR,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRUIT

BRIEF OF AMICI CURIAE ELECTRONIC PRIVACY INFORMATION CENTER, AMERICAN CIVIL LIBERTIES UNION, AMERICAN LIBRARY ASSOCIATION, ASIAN AMERICAN LEGAL DEFENSE AND EDUCATION FUND, CENTER FOR DEMOCRACY AND TECHNOLOGY, CONSUMER PROJECT ON TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, NATIONAL CONSUMERS LEAGUE, PRIVACY RIGHTS CLEARINGHOUSE, PRIVACYACTIVISM, U.S. PUBLIC INTEREST RESEARCH GROUP, AND 16 LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF PETITIONER

MARC ROTENBERG
Counsel of Record
DAVID L. SOBEL
CHRIS JAY HOOFNAGLE
MARCIA HOFMANN
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140

August 25, 2003

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE AMICI CURIAE 1

SUMMARY OF THE ARGUMENT 5

ARGUMENT 6

I. THE WRONGFUL DISCLOSURE OF THE SOCIAL SECURITY NUMBER CREATES AN ONGOING PRIVACY RISK 6
- A. The Historical Use of the SSN 7
- B. Harms from SSN Disclosure in Recent Years 9

II. LIQUIDATED DAMAGE PROVISIONS ARE A LONG-STANDING TECHNIQUE TO PROVIDE REMEDIES FOR PRIVACY VIOLATIONS 13
- A. Privacy Scholars Recognize the Critical Role of Liquidated Damage Provisions in Privacy Statutes 14
- B. Liquidated Damage Provisions are Routinely Included in Statutory Privacy Laws 16

III. THE FOUNDATIONAL 1973 REPORT, THE 1974 ACT, AND THE 1975 AGENCY GUIDELINES ALL INTENDED THAT THE PRIVACY ACT WOULD PROVIDE LIQUIDATED DAMAGES 18
- A. The HEW Advisory Committee Report of 1973 18
- B. Legislative History of the Privacy Act of 1974 23
- C. The OMB Guidelines of 1975 28

CONCLUSION 29

TABLE OF AUTHORITIES

Cases

Buckhannon Bd. & Care Home, Inc. v. West Virginia Dep't of Health & Human Servs., 532 U.S. 589 (2001). .14

Chevron U.S.A., Inc. v. NRDC, 467 U.S. 837 (1984) . . . 29

Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993). 7

Statutes

5 U.S.C. § 552a(g)(1)(D) 29

5 U.S.C. § 552a(v) 29

12 U.S.C. § 3417(a)(1) 18

18 U.S.C. § 2520(c)(1)(A) 16, 17

18 U.S.C. § 2520(c)(1)(B) 17

18 U.S.C. § 2520(c)(2)(B) 17

18 U.S.C. § 2707(c) 17

18 U.S.C. § 2710 16

18 U.S.C. § 2710(c)(2)(A) 16

18 U.S.C. § 2721 16

18 U.S.C. §2724(a) 16

18 U.S.C. §2724(b)(1) 16

47 U.S.C. § 551(f)(2)(A) 17

47 U.S.C. § 2724(b)(1) 17

Pub. L. 93-579, codified at 5 U.S.C. § 552a 8

Pub. L. 93-579, § 7 . . . . . 8, 28

Pub. L. 93-579, § 7(b) 8

Legislative Materials

Staffs of Senate Comm. On Government Operations and House Comm. On Government Operations, 94th Cong., *Legislative History of the Privacy Act of 1974 – S. 3418 (Public Law 93-579)* (Joint Comm. Print 1976) 8, 23, 24, 25, 26, 27 28

S. Rep. No. 93-1183 (1974) 8, 23, 24

S. 3418, 93d Cong. §304(b) (1974) 23, 25, 26

H.R. 16373, 93d Cong. §304(b) (1974) 23, 24, 27

Miscellaneous Sources

Frank P. Anderano, *The Evolution of Federal Computer Crime Policy*, 27 Am. J. Crim. L. 81 (1999) 15

A To-Don't List For the New Year, How to Fix Your Life in 2003, Wall St. J., Dec. 31, 2002 12

Mark E. Budnitz, *Privacy Protection For Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. Rev. 847 (1998) 14

CALPIRG & Privacy Rights Clearinghouse, *Nowhere to Turn: Victims Speak Out on Identity Theft* (2000) . . 12, 13

Abram Chayes, *The Role of the Judge in Public Law Litigation,* 89 Harv. L. Rev. 1281 (1976) 13

Dep't. of Health, Educ. and Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (Washington, D.C., Government Printing Office 1973) 8, 18, 19, 20, 21, 22

Jonathan L. Entin, *The Right to Privacy One Hundred Years Later: Privacy Rights and Remedies*, 41 Case W. Res. L. Rev. 689 (1991) 14, 15

Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Senate Judiciary Committee, 92d Cong., 1st Sess. Part I (1971) 20, 21

Federal Trade Commission, *ID Theft: When Bad Things Happen to Your Good Name* (2002) 12

Fraud Charges Jump in 2002 on Consumer Complaints, ID Thefts, Electronic Com. & L. Rep., Vol. 8(4) (Jan. 29, 2003) 10

Robert Gellman, *Does Privacy Law Work? in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193 (Philip E. Agre & Marc Rotenberg, eds.) 10

General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (2002). 10

General Accounting Office, *Privacy Report*, Vol. 2, No. 28 (July 14, 2003) 9

General Accounting Office, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (2002) 9

Identity Theft in Florida, Sixteenth Statewide Grand Jury Report, SC 01-1095, Supreme Court of Florida, Jan. 10, 2002, *at* http://www.idtheftcenter.org/attach/ FL_idtheft_gj.pdf 11, 12

Information on Identity Theft for Consumers and Victims from January 2002 Through December 2002, Fed. Trade Commission Rep., *available at* http://www.consumer.gov/ idtheft/reports/ CY2002ReportFinal.pdf 10

Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998) 16

Frederick Lodge, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 Fordham L. Rev. 611 (1984) 13

Office of Management and Budget, *Guidelines for Implementing Section 552a of Title 5 of the United States Code*, (1975) 28, 29

Social Security Administration, *Frequently Asked Questions*, *available at* http://www.ssa.gov/history/hfaq.html 7

Social Security Administration, *Regulation No. 1* (adopted July 11, 1936), available at http://www.ssa.gov/history/reg.1.htm 7

Social Security Administration Office of the Inspector General, *Social Security Number Misuse*, June 2003, *available at* http://www.ssa.gov/oig/executive_operations/factsheet1.htm. 11

Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227 (2003) 15

Testimony of Barbara Bovbjerg, Director of Education, Workforce, and Income Security Issues, General Accounting Office *Social Security Numbers: Ensuring the Integrity of the SSN, Hearing before the* House Social Security Subcommittee of the Ways and Means Committee (2003) 9

R. Turn and W.H. Ware, *Privacy and Security Issues in Information Systems*, in ETHICAL ISSUES IN THE USE OF COMPUTERS (Deborah G. Johnson & John W. Snapper eds., 1985) 20

Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890) 13

ALAN F. WESTIN AND MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY, (1972) 21

Jay Weiser, *Measure of Damages for Violation of Property Rules: Breach of Confidentiality*, 9 U. Chi. L. Sch. Roundtable 75 (2002) 14

INTEREST OF THE AMICI CURIAE [1]

All *amici curiae* represented in this brief have a significant interest in the effective enforcement of privacy laws in the United States. The groups also share a common concern regarding the increase in identity theft, a crime that is facilitated by the misuse of the Social Security Number.

Amici Privacy, Consumer, and Civil Liberties Organizations

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established in 19994 to focus public attention on emerging civil liberties issues. EPIC has participated as *amicus curiae* in numerous privacy cases, including *Smith v. Doe*, 123 S. Ct. 1140 (2003), *Dep't. of Justice v. City of Chicago*, 123 S. Ct. 1352 (2003), *Watchtower Bible and Tract Soc'y of N.Y. Inc. v. Vill. of Stratton*, 536 U.S. 150 (2002), and *Reno v. Condon*. 528 U.S. 141 (2000).

The American Civil Liberties Union ("ACLU") is the largest civil liberties organization in the United States, with approximately 400,000 members. Over its 83-year history, the ACLU has consistently defended the principles of liberty enshrined in the Bill of Rights, including the right to privacy.

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6 it is stated that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party. Law school students participating in the EPIC Internet Public Interest Opportunities Program (IPIOP) Erik J. Blum, Eva Gutierrez, Sherwin Siy, Tiffany A. Stedman, and Maryam Zafar assisted in the preparation of the brief.

The American Library Association ("ALA"), founded in 1876, is the oldest and largest library association in the world. With a membership of more than 64,000 librarians, library trustees, library educators, friends of libraries and other interested persons from every state, ALA is the chief advocate for the people of the United States in their search for the highest quality of library and information services.

The Asian American Legal Defense and Education Fund ("AALDEF"), founded in 1974, promotes and protects the civil rights and civil liberties of Asian Americans through litigation, advocacy and community education. AALDEF is particularly concerned about the privacy rights of immigrants and new citizens.

The Center for Democracy and Technology is a non-profit public interest organization in Washington, D.C. dedicated to promoting civil liberties in this age of digital technologies, including advocating strong privacy protections for personal information in government databases.

The Consumer Project on Technology is a non-profit organization created by Ralph Nader to investigate consumer concerns relating to new technologies.

The Electronic Frontier Foundation is a non-profit, civil liberties organization based in San Francisco, California that works to protect privacy and free speech rights in the digital world.

The National Consumers League, the nation's oldest consumer organization, is a private, nonprofit advocacy group representing consumers on marketplace and workplace issues.

Privacyactivism is a non-profit organization whose goal is to enable people to make well-informed decisions

about the importance of privacy on both a personal and societal level

The Privacy Rights Clearinghouse is a nonprofit consumer education, research, and advocacy organization, established in 1992 and based in San Diego, California.

The U.S. PIRG serves as the national association of state Public Interest Research Groups. PIRGs are non-profit, non-partisan public interest advocacy groups. The PIRGs have a longstanding interest in privacy protection, and have recently published several major reports on the problems of identity theft, which is exacerbated by easy access to Social Security Numbers.

Amici Legal Scholars and Technical Experts

Anita L. Allen, Professor of Law and Philosophy, University of Pennsylvania

Ann Bartow, Assistant Professor of Law, University of South Carolina School of Law

James Boyle, William Neal Reynolds Professor of Law, Duke University Law School

Susan Freiwald, Professor of Law, University of San Francisco School of Law

Llewellyn Joseph Gibbons, Associate Professor, College of Law, University of Toledo

Jerry Kang, Visiting Professor of Law, Harvard Law School

Ian R. Kerr, Canada Research Chair in Ethics, Law & Technology, Faculty of Law, Common Law Section, University of Ottawa

Dr. Peter G. Neumann, Principal Scientist, SRI International Computer Science Laboratory

Malla Pollack, Visiting Associate Professor Law, University of Chicago School of Law

Pamela Samuelson, Chancellor's Professor of Law and Information Management, University of California, Berkeley

Dr. Bruce Schneier, Chief Technical Office, Counterpaine Internet Security

Paul M. Schwartz, Professor of Law, Brooklyn Law School.

Dr. Barbara Simons, Former President, Association for Computing Machinery

Daniel J. Solove, Visiting Associate Professor, George Washington University School of Law

Lior J. Strahilevitz, Assistant Professor of Law, University of Chicago Law School

Katherine J. Strandburg, Assistant Professor of Law, DePaul College of Law

SUMMARY OF THE ARGUMENT

At issue in this case is whether a plaintiff suing under the Privacy Act of 1974, 5 U.S.C. § 552a, for the wrongful disclosure of the Social Security Number must show actual damages in order to recover the statutory damages of $1,000.

Social Security Number disclosures may result in serious harms. This is because the Social Security Number is used as an identification code for databases containing a wide range of financial, medical, educational, and credit information. It is like a master key that opens many doors. Public safety and personal privacy require that the distribution of the SSN be carefully controlled.

The civil remedy provision in the Privacy Act, like many similar provisions in other privacy statutes, provides for the recovery of either actual damages or statutory damages where intentional violations of the Act occur. Congress has long incorporated liquidated damages provisions in privacy statutes to ensure enforcement of such statutes, promote judicial economy, and provide a specified remedy where it would otherwise be difficult or impracticable to determine monetary damages. The need to provide such a remedy is particularly important in privacy cases, where scholars and the courts have long recognized the difficulty in quantifying harm.

The legislative history of the Privacy Act, as well as a significant government report that provided the basis for the Act, make clear Congress's intent to limit the use of the Social Security Number and to provide meaningful remedies for misuse. Congress explicitly recognized the particular risk to privacy that could result from such disclosures and thus provided a damages provision that would enable the public to

enforce the legal protections against wrongful Social Security Number disclosure.

With the growing threat of identity theft and the significant risk of misuse of the Social Security Number, it is particularly important for the Court to ensure effective enforcement of the Act and to interpret the liquidated damages provision as Congress intended. The crabbed reading of the key statutory language by the court below – one that has been rejected by virtually all the other circuits – should be rejected.

ARGUMENT

Consideration of the petitioner's claim – that intentional or willful disclosure by the government of the Social Security Number ("SSN") automatically entitles the plaintiff to the $1,000 statutory damages – requires an appreciation of the significant harms that can occur with the disclosure of the SSN, the history of liquidated damages in general, and the intent of Congress in enacting these provisions, as evidenced by the legislative history.

I. The Wrongful Disclosure of the Social Security Number Creates an Ongoing Privacy Risk

Central to the protection of privacy in our modern society are the provisions in the Privacy Act of 1974 that seek to limit both the tangible and intangible harms that flow from the wrongful disclosure of the Social Security Number. As Judge Michael wrote in partial dissent in the decision below, an individual can be adversely affected before any crime occurs due to distress about possible misuse of his illegally disclosed SSN. 306 F.3d 170, 185 (4th Cir. 2002) (Michael, J., dissenting). As the Fourth Circuit earlier stated

in *Greidinger v. Davis,* "the harm that can be inflicted from the disclosure of an SSN to an unscrupulous individual is alarming and potentially financially ruinous." 988 F.2d 1344, 1354 (4th Cir. 1993). Numerous studies demonstrate the risk of harm that results from the wrongful disclosure of the SSN, as well as the practical problems that may arise in trying to quantify privacy harms. The statutory damage provision in the Privacy Act recognizes these risks and specifically seeks to prevent the misuse of the Social Security Number, even in the absence of proof of actual damages.

A. The Historical Use of the SSN

The SSN was established in 1936 as a nine-digit account number to "to facilitate the early manual bookkeeping operations associated with the creation of Social Security in the 1930s." Social Security Administration, *Frequently Asked Questions*, *Q18, available at* http://www.ssa.gov/history/hfaq.html. Because of the importance placed on privacy in the Social Security program, the very first regulation adopted by the new Social Security Board in June 1937 was its rules regarding confidentiality of its records. Social Security Administration, *Regulation No. 1* (adopted July 17, 1936), *available at* http://www.ssa.gov/history/reg1.html. A special effort was made to limit the use of the Social Security Number for purposes unrelated to the administration of the program. The Social Second card, as published by the federal government in 1946, bore the words "For Social Security Purposes - Not for Identification." Social Security Administration, *Frequently Asked Questions*, *Q21, available at* http://www.ssa.gov/history/hfaq.html.

Over time, however, SSNs were used for purposes unrelated to the administration of the Social Security system. For example, in 1961 Congress authorized the Internal

Revenue Service to use SSNs as taxpayer identification numbers. Dep't. of Health, Educ. and Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 114 (Government Printing Office 1973) [hereinafter "HEW Report"]. Public concerns about the automation of personal information in government agencies began to grow. In response to the recommendations contained in the HEW Report and the growing risks associated with the accumulation of massive amounts of personal information, Congress passed the Privacy Act of 1974. Pub. L. 93-579, codified at 5 U.S.C. § 552a. Among other things, the Privacy Act makes it unlawful for a governmental agency to deny a right, benefit, or privilege merely because the individual refuses to disclose his SSN. Pub. L. 93-579, § 7.

When the Privacy Act was enacted, Congress recognized the dangers of widespread use of SSNs as universal identifiers. Section 7 of the Privacy Act provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." Pub. L. 93-579, § 7(b). In support of this provision, the Senate Committee on Government Operations stated that the widespread use of SSNs as universal identifiers was "one of the most serious manifestations of privacy concerns." S. Rep. No. 93-1183 at 28, *reprinted in* Staffs of Senate Comm. on Government Operations and the House Comm. on Government Operations, 94th Cong., *Legislative History of the Privacy Act of 1974 – S. 3418 (Public Law 93-579)* 181 (Joint Comm. Print 1976) [hereinafter "Legislative History"].

B. Harms from SSN Disclosure in Recent Years

The use of the SSN has expanded significantly since the Privacy Act was enacted in 1974. A recent General Accounting Office ("GAO") study found that government and some private entities rely extensively on SSNs, increasing the availability of these numbers to the public. *Privacy Report*, Vol. 2, No. 28 (July 14, 2003). This study also identified numerous examples of public and private databases that were compromised and SSNs that were stolen. *Id*. In some cases, the display of SSNs in public records and unprotected Web sites fostered identity theft. *Id*.

The GAO has also recognized the risk of identity theft via SSN disclosure. General Accounting Office, *Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards*, GAO-02-352 (2002). This report notes that along with names and birth certificates, SSNs are among the three most sought-after identifiers by identity thieves. *Id*. at 13 (*citing* United States Sentencing Commission, *Identity Theft Final Alert* (1999)). The GAO also noted that identity theft is on the rise, with the Social Security Administration receiving 11,000 complaints of SSN misuse in fiscal year 1998, but more than 65,200 such complaints in fiscal year 2001. *Id*. at 14.

The increasing number of complaints is accompanied by rising costs to individuals. Consumers reported losses from fraud totaling more than $343 million in 2002. Testimony of Barbara Bovbjerg, Director of Education, Workforce, and Income Security Issues, General Accounting Office, *Social Security Numbers: Ensuring the Integrity of the SSN, Hearing before the House Social Security Subcommittee of the Ways and Means Committee* (2003) at 3. Identity theft accounts for over 80 percent of SSN misuse. *Id*.

However, many of the problems resulting from the misuse of the SSN cannot easily be quantified as actual damages. Data collected by the Federal Trade Commission ("FTC") and compiled by the GAO highlight the non-monetary losses suffered by individuals whose identities have been stolen. General Accounting Office, *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 at 55 (2002). Non-monetary losses were common. Of a sampling of 77,316 identity theft victims, 13,357 reported non-monetary harms as defined by the FTC. *Id*. at 56. Included as non-monetary costs were harms such as victims being denied credit or other financial services (7,376 victims); lost time due to resolving problems (3,489); being unjustly harassed by debt collectors or creditors (2,968); being subjected to criminal investigation, arrest, or conviction (1,281); having a civil suit filed or judgment entered against them (819); and being denied employment or losing their jobs (580 victims). *Id*.

The FTC reported, based on victim-initiated complaints to the agency, a large increase in the number of identity theft cases in the last year and a doubling of the dollar loss attributable to fraudulent activities directed at U.S. consumers. *Fraud Charges Jump in 2002 on Consumer Complaints, ID Thefts*, Electronic Com. & L. Rep., Vol. 8(4), Jan. 29, 2003. The agency noted that the number of fraud complaints rose from 220,000 in 2001 to 380,000 in 2002 and the loss to consumers grew from $160 million in 2001 to $343 million in 2002. *Id*. The report revealed that identity theft topped the list of consumer complaints filed with the FTC, accounting for forty-three percent of the complaints lodged in the Consumer Sentinel database. *Id*. Furthermore, the most recent identity theft data from the Federal Trade Commission shows that seventy-two percent of victims do

not know how the thief obtained their personal information. *Information on Identity Theft for Consumers and Victims from January 2002 Through December 2002*, Fed. Trade Commission Rep. at 8, *available at* http://www.consumer.gov/idtheft/reports/CY2002ReportFinal.pdf.

The link between crime, and possibly even terrorist acts, and the availability of the SSN is so strong that the Social Security Administration ("SSA") recently warned: "The SSN is a valuable commodity for criminals at all levels, as it allows individuals to integrate themselves into our society with relative anonymity and commit crimes or acts of terrorism, while avoiding detection." Social Security Administration Office of the Inspector General, *Social Security Number Misuse*, June 2003, *available at* http://www.ssa.gov/oig/executive_operations/factsheet1.htm. The SSA further reported that fifty-eight percent of its fiscal year 2002 complaints involved SSN misuse. *Id*. Given the growing urgency of the problem, the agency recommended that Congress "[p]rohibit the sale of SSNs, prohibit their display on public records, and limit their use to valid transactions." *Id.*

Similar concerns about the growing misuse of the SSN have been expressed at the state level. In January 2002, a special Florida grand jury commissioned to investigate identity theft recommended stronger legal protections for personal data, including SSNs, held by business and state agencies. *Identity Theft in Florida*, Sixteenth Statewide Grand Jury Report, SC 01-1095, Supreme Court of Florida (Jan. 10, 2002) *at* http://www.idtheftcenter.org/attach/FL_idtheft_gj.pdf. The grand jury called for laws that would stop State agencies from disseminating personal information under the open records law without individual consent, court order, or the articulation of a compelling need. *Id.* The grand

jury estimated that the current $2.5 billion nationwide cost of identity theft is expected to grow to $8 billion by 2005. *Id*. It found that the financial services industry loses $17,000 per compromised identity. It cited health clubs and video rental stores requiring SSNs on applications and local governments asking for SSNs on routine transactions as a cause of identity theft. *Id*.

Because of the risk of identity theft associated with revealing the SSN, the Wall Street Journal recently advised readers not disclose their SSN: "Don't give out your Social Security number unless you have to: With identity theft a growing problem, you should be extremely cautious about giving out that information." *A To-Don't List For the New Year, How to Fix Your Life in 2003,* Wall St. J., Dec. 31, 2002. *See also* Federal Trade Commission, *ID Theft: When Bad Things Happen to Your Good Name* 3 (2002) ("Give your SSN only when absolutely necessary . . . Don't carry your SSN; leave it in a secure place . . .), *available at* ttp://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm.

A report from two leading consumer organizations also makes clear the risk that the misuse of the Social Security Number can contribute to identity theft. "Many victims complained that easy access to their Social Security numbers made it easy for identity thieves to impersonate them." CALPIRG & Privacy Rights Clearinghouse, *Nowhere to Turn: Victims Speak Out on Identity Theft* 17 (2000). The consumer organizations also found that the harms were often not easy to quantify:

> Although the fraud committed against the victims surveyed totaled as much as $200,000, the common themes were that stress, emotional trauma, time lost, and damaged

> credit reputation – not the financial aspect of the fraud – were the most difficult problems. One victim from Nevada explained, "(T)his is an extremely excruciating and violating experience, and clearly the most difficult obstacle I have ever dealt with."

Id. at 4.

The growing risk of identity theft, based in part on the misuse of the Social Security Number, is precisely the type of adverse effect that the Privacy Act seeks to limit. A requirement for showing actual damages in this context would effectively frustrate the purposes of the Act.

II. Liquidated Damage Provisions Are a Long-Standing Technique to Provide Remedies for Privacy Violations

Tort law has long provided remedies for intangible harms**,** such as those resulting from defamatory statements or torts against dignity. Abram Chayes, *The Role of the Judge in Public Law Litigation,* 89 Harv. L. Rev. 1281, 1283 (1976). Violation of privacy is such an intangible harm that has become increasingly significant in tort law. A central problem in privacy cases is the difficulty for the injured party to demonstrate actual damages. Frederick Lodge, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 Fordham L. Rev. 611, 612 (1984). This problem was well understood by Samuel Warren and Louis Brandeis, the authors of the famous article that provided the basis for the privacy tort. *The Right to Privacy*, 4 Harv. L. Rev. 193, 219 (1890) ("Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel.")

Thus, in order to compensate the victim and recognize that a harm was committed, though it may be difficult to quantify, privacy statutes routinely include liquidate damage provisions. While the actual language providing statutory damages varies, there is no significant difference in the purpose. As Justice Scalia wrote in concurrence in *Buckhannon Bd. & Care Home, Inc. v. West Virginia Dep't of Health & Human Servs.*:

> [I]t would be no more rational to reject the normal meaning of 'prevailing party' because some statutes produce the same result with different language, than it would be to conclude that, since there are many synonyms for the word 'jump,' the word 'jump' must mean something else.

532 U.S. 589, 614-15 (2001) (Scalia, J., concurring). Where there is an intentional violation of a privacy statute, awards of such damages ensure compensation for the victim, deter future violations, and promote judicial economy by reducing the need for difficult determination of harm in cases.

A. Privacy Scholars Recognize the Critical Role of Liquidated Damage Provisions in Privacy Statutes.

Scholars have argued that the purpose of liquidated damages in privacy statutes is not only to compensate the victim for an intangible harm, but also to provide enforcement of such statutes. *See, e.g.,* Mark E. Budnitz, *Privacy Protection For Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. Rev. 847, 883 (1998). Professor Jay Weiser has written that federal privacy statutes attempt to resolve the difficulty in calculating damages through liquidated damages provisions,

which in turn saves enforcement costs. Jay Weiser, *Measure of Damages for Violation of Property Rules: Breach of Confidentiality*, 9 U. Chi. L. Sch. Roundtable 75, 100 (2002). Liquidated damage provisions also relieve juries of difficult damages determinations. Jonathan L. Entin, *The Right to Privacy One Hundred Years Later: Privacy Rights and Remedies*, 41 Case W. Res. L. Rev. 689, 693 (1991). Thus, highly discretionary calculations are unnecessary. The purpose of statutory damages is both to encourage a victim to pursue a case under a privacy statute and to serve as a deterrent to would-be violators. Frank P. Anderano, *The Evolution of Federal Computer Crime Policy*, 27 Am. J. Crim. L. 81, 98 (1999).

Professor Daniel J. Solove points to another reason to ensure that restrictions on the misuse the SSN are effectively enforced: victims often do not know when a breach has occurred:

> Victims are often unaware that their identities have been stolen until long after the identity theft has begun. A report based on victim surveys estimates that it takes victims over a year to discover they have been victimized. According to FTC estimates, 20% of identity theft victims learn of the theft after two years.

Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1248 (2003). Solove further suggests that the costs of identity theft are also borne by other than those who are the targets. "[B]eyond losses to particular individuals, identity theft results in losses to creditors, financial institutions, and companies, and these losses are passed down to consumers in the form of higher interest rates, prices, and fees." *Id.* at 1246.

Scholars also consider the inclusion of liquidated damage provisions important for effective privacy laws in such new areas as the Internet. For example, Professor Jerry Kang has set out a model "Cyberspace Privacy Act" which provides that: "The court may award actual damages but not less than liquidated damages computed at the rate of $100 for each separate violation or $5000, whichever is higher." Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1293 (1998).

B. Liquidated Damage Provisions are Routinely Included in Statutory Privacy Laws

Numerous privacy statutes contain liquidated damages provisions to both compensate the victim and deter future violations. For example, the Video Privacy Protection Act ("VPPA") and the Drivers Privacy Protection Act ("DPPA") provide for a statutory damage award where intentional violations of the acts occur. 18 U.S.C. § 2710; 18 U.S.C. § 2721. The VPPA provides that "the court may award actual damages but not less than liquidated damages in an amount of $2,500." 18 U.S.C. § 2710(c)(2)(A). In essentially the same language, the DPPA provides that "the court may award (1) actual damages, but not less than liquidated damages in the amount of $2,500" against "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter[.]" 18 U.S.C. § 2724(b)(1), (a).

Similarly, the Electronic Communications Privacy Act of 1986 ("ECPA") establishes statutory damage awards, depending on the type of violation. For example, in relation to the interception of electronic communications, ECPA provides that "if the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has

not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and no more than $500." 18 U.S.C. § 2520(c)(1)(A). The court is required to award statutory damages of no less than $100 and no more than $1,000 for victims of those who have violated ECPA on a previous occasion. 18 U.S.C. § 2520(c)(1)(B). For more than two violations of ECPA, the statute provides that:

> [I]n any other action under this section, the court may assess as damages whichever is the greater of (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

18 U.S.C. § 2520(c)(2)(B). Furthermore, regarding unlawful access to stored communications, ECPA provides that the court may assess actual damages suffered by the plaintiff and profits made by the violator as a result of the violation, "but in no case shall a person entitled to recover receive less than the sum of $1,000." 18 U.S.C. § 2707(c).

There are many other privacy statutes that provide liquidated damages. The Cable Communications Policy Act ("CCPA"), which protects the privacy of cable television subscribers, provides that "the court may award actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher." 47 U.S.C. § 551(f)(2)(A). The Telephone Consumer Protection Act ("TCPA"), a privacy statute that protects individuals from constant telemarketing,

also provides statutory damages: "the court may award actual damages, but not less than liquidated damages in the amount of $2,500." 47 U.S.C. § 2724(b)(1). Additionally, under the Right to Financial Privacy Act of 1974 ("RFPA"), which was enacted the same year as the Privacy Act provision now before the Court, a successful plaintiff may collect $100 per RFPA violation from the defendant. 12 U.S.C. § 3417(a)(1).

As the drafters of the Privacy Act and privacy statutes enacted since understood, liquidated damage provisions are an essential requirement for meaningful privacy protection.

III. The Foundational 1973 Report, the 1974 Act, and the 1975 Agency Guidelines All Intended that the Privacy Act would Provide Liquidated Damages

The history of the Privacy Act indicates a clear intent to provide liquidated damages where a violation occurs. The federal advisory committee report that preceded the Act recommended liquidated damages; the OMB Guidelines that implemented the Act provided for liquidate damages. The final language in the Act incorporated the liquidated damages provision drafted in the Senate and agreed to by the House.

A. The HEW Advisory Committee Report of 1973

The Privacy Act of 1974 was enacted out of a growing concern for the rights of citizens in the face of advancing technology. The Act was the legislative culmination of extensive academic research that revealed the many threats to individual privacy and autonomy in the wake of increasingly powerful computer databases. One of the most influential studies to which the Congress looked when drafting the Privacy Act was the 1973 report *Records, Computers, and the Rights of Citizens*, prepared for the Department of Health, Education and Welfare ("HEW

Report"). The federal advisory committee that produced the report sought to determine the limitations that should be placed on the application of computer technology to record keeping about citizens. *Id.* at 33. The advisory committee foresaw that sensitive or personal information could be compromised when compiled into vast databases that lacked regulatory oversight. *Id.* at 28. Ultimately, the HEW Report outlined a series of recommendations that became the basis of the Privacy Act of 1974.

To address the lack of privacy protections in automated record keeping systems, the HEW Report recommended the enactment of legislation establishing a Code of Fair Information Practices that would govern all automated personal data systems. *Id*. at 50. The Code articulated basic informational privacy principles, and allocated rights and responsibilities in the collection and use of personal information. *Id*. The Code of Fair Information Practices proposed by the HEW Report provides:

> - There must be no personal-data record-keeping systems whose very existence is secret.
> - There must be a way for an individual to find out what information about him is in a record and how it is used.
> - There must be a way for an individual to prevent information obtained about him for one purpose from being used or made available for other purposes without his consent.
> - There must be a way for an individual to correct or amend a record of identifiable information about him.

> • Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

Id. at 41.

These highly influential principles formed the basis of the Privacy Act of 1974 and many privacy laws since. R. Turn and W.H. Ware, *Privacy and Security Issues in Information Systems*, in ETHICAL ISSUES IN THE USE OF COMPUTERS 133, 138 (Deborah G. Johnson & John W. Snapper eds. 1985). See also Robert Gellman, *Does Privacy Law Work? in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 196 (Philip E. Agre & Marc Rotenberg, eds.) ("The articulation of principles of fair information practices may be the computer age's most significant policy development with respect to privacy.").

Of particular concern to the advisory committee was the increasing ease with which personal information could be linked to an individual by means of Standard Universal Identifier ("SUI"). HEW Report at 112. Public opposition during the 1960s to the misuse of the Social Security Number was evident during a series of hearings held on privacy and information collection. *See, e.g., Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Senate Judiciary Committee*, 92d Cong., 1st Sess. Part I, 775-881 (1971). As HEW Secretary Elliot Richardson testified in 1971:

> There would certainly be an enormous convenience in having a single identifier for

> each individual . . . [making] more efficient the acquisition, storage, and use of data . . . . It is the very ease of assembling complete records, of course, which raises the specter of invasion of privacy.

Id. at 784. *See also* ALAN F. WESTIN AND MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY 399 (1972) ("adopting the Social Security number officially as a national identifier or letting its use spread unchecked cannot help but contribute to public distrust of government").

Thus, in addition to outlining broad recommendations to safeguard personal information in automated personal data systems, the HEW advisory committee also recommended against the adoption of any standardized identifier, whether the SSN or otherwise, that would "enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government and government-supported automated personal data systems." HEW Report at xxxiii. The advisory committee specifically recommended against the use of the SSN for generalized record keeping:

> Accordingly, we recommend . . . [t]hat any organization or person required by Federal law to obtain or record the SSN of any individual from making any use or disclosure of the SSN without the informed consent of the individual, except as may be necessary to the Federal government purposes for which it was required to be obtained and recorded. This prohibition should be established by a specific and preemptive act of Congress.

Id. at 130-31. The committee foresaw that the use of the SSN as a means of record keeping–for example, as case numbers

in compensation claims as in this case–was directly at odds with the protections due such a sensitive identifier. *Id*. at 30. The committee's recommendation was "intended to constrain the behavior of organizations and persons that are legally required to obtain and record the SSN for federal purposes, but which use the SSN in other ways that constitute virtual public dissemination." *Id.*

The HEW Report also recommended strong legal remedies for privacy violations. *Id*. at 36. "Unless injury to the individual can be translated into reasonably substantial claims for damages, the individual ordinarily has little incentive to undertake a lawsuit. Few people can afford to bring suit against a well-defended organization solely for moral satisfaction." *Id.* The advisory committee recommended "the enactment of legislation establishing a Code of Fair Information Practices for all automated personal data systems." *Id*. at 50. Regarding violations of the Act, the HEW Report said:

> The Code should give individuals the right to bring suits for unfair information practices to recover actual, *liquidated*, and punitive damages, in individual and class actions. It should also provide for recovery of reasonable attorney's fees and other costs of litigation incurred by individuals who bring successful suits.

Id. (emphasis added). The Privacy Act, enacted a year after the HEW Report was released, implemented many of the advisory committee's recommendations, including restrictions on the use of the Social Security Number and liquidated damages for violations of the Act.

B. Legislative History of the Privacy Act of 1974

The civil remedy provision in the Privacy Act was as a compromise between the Senate bill, which held the government liable regardless of culpability and provided for both actual and general damages, with liquidated damages of $1,000; and the House bill, which required that the violation be "willful, arbitrary, or capricious" before awarding only actual damages. The compromise retains the $1,000 in liquidated damages in lieu of general damages, but allows this recovery and actual damages only if the violation is "intentional or willful."

1. Statutory Damages

The original Senate bill, S. 3418, introduced in the Senate Committee on Government Operations, provided for both actual and punitive damages for any violation of the Privacy Act. S. 3418, 93d Cong. §304(b) (1974), *reprinted in* Legislative History at 27. The parallel House bill, H.R. 16373, originally provided for actual damages in all cases, with additional punitive damages if the violation was "willful, arbitrary, or capricious." H.R. 16373, 93d Cong. §304(b) (1974), *reprinted in* Legislative History at 250-51. From the outset, Congress recognized that violations of an individual's privacy required compensation beyond actual, out-of-pocket expenses.

After S. 3418 was introduced, the Senate Committee on Government Operations issued a report noting the Committee's intention that a person should have a cause of action for a denial of access, without having to show a particular injury or denial of benefits. S. Rep. No. 93-1183 at 82 (1974), *reprinted in* Legislative History at 235. The Committee also noted that it is often "exceedingly difficult for a citizen . . . to establish a 'cause and effect' relationship

between the information in his file and some subsequent damage to him." *Id*. In addition, the Committee stated that, since the Privacy Act did not grant enforcement authority to any administrative body, the legislation should encourage "the widest possible citizen enforcement through the judicial process." *Id*. at 83, *reprinted in* Legislative History at 236.

The House Committee on Government Operations reported out H.R. 1673 on September 24, but removed the provision on punitive damages. Representatives Abzug, Moss, Stanton, Gude, Burton, Fascell, Culver, Collins, Rosenthal, and Conyers expressed concern about the absence of punitive damages, proposed in the House measure, since "[a]ctual damages resulting from an agency's misconduct will, in most cases, be difficult to prove and this will often preclude an adequate remedy at law." Legislative History at 330. The representatives considered the inclusion of punitive damages, "or, at the very least, *liquidated damages*," to be "essential." *Id* (emphasis added).

Representative Fascell unsuccessfully offered an amendment to essentially restore the original damages language of H.R. 16373. *Id*. at 919. This amendment would have made actual damages available for all violations of the Privacy Act, with punitive damages for willful, arbitrary, or capricious violations. *Id*. at 919-20. Representative McCloskey opposed this amendment. He was concerned about subjecting the United States to potentially limitless punitive damages. *Id*. at 922. Representative Eckhardt pointed out that in the absence of the Fascell amendment, a person who had suffered any amount of actual damage because of the negligence of an agency would be unable to recover. *Id*. The Fascell amendment was ultimately rejected, as it was identical to language rejected by the committee

below. *Id*. at 924.] After additional debate, the bill was passed by the House. *Id*. at 983.

That same day, the Senate considered S. 3418 as reported out by the Committee on Government Operations. *Id.* at 763. The Committee offered several amendments to the bill, which at the time allowed a plaintiff to sue the individual agent responsible for the Privacy Act violation. *Id.* at 768. Instead, the Committee recommended that only the agency be liable, and that the plaintiff should be able to recover both actual and general damages, with a provision for liquidated damages "of say $1,000." *Id*. The bill was thus passed providing for actual and general damages, and the liquidated damages suggestion incorporated as "but in no case shall a person entitled to recovery receive less than the sum of $1,000." *Id*.

The provision in the Act as passed that no person recovering should receive less than $1,000 clearly stems from the Senate Committee's recommendation for liquidated damages—the language is identical.

The Senate reduced the standard of culpability to "willful or intentional," which was thought to be easier for a plaintiff to show than the House's "willful, arbitrary, or capricious," but greater than "gross negligence." *Id*. at 862. The House's language on actual damages was retained, but with the Senate's liquidated damages clause of $1,000. The final measure, agreed to by both houses, provided for liquidated damages where a willful or intentional violation of the Act occurred.

2. Social Security Number

Concerns about the use of the SSN as a universal identifier were prevalent throughout the history of the Privacy Act's passage. The original S. 3418 explicitly made

it unlawful for anyone to require the disclosure or furnishing of an SSN, except as required under the Social Security Act in the administration of benefits. Legislative History at 23. This provision was debated and eventually eliminated during markup. *Id*. at 68.

On September 19, 1974, Senator Goldwater, with Senator Percy, introduced an amendment that, while allowing existing uses of the SSN, prevented its use in future systems. *Id*. at 761. The amendment covered not only government uses, but also prevented "any person" from discriminating against an individual "in the course of any business or commercial activity" because of refusal to disclose the SSN. *Id*. Senator Goldwater's comments touched on two main concerns: first, that individuals would be reduced to their identifying numbers; and second, that this number, linked, could mean that a person would "leave a trail of personal data behind him for all his life which could be immediately reassembled to confront him." *Id*. at 759-60. Senator Percy cited the HEW Report's recommendations in support of this amendment. *Id*. at 762.

This amendment to S. 3418 was considered and accepted by the House on November 21. *Id*. at 804. Prior to the amendment's consideration on the floor, Senator Percy noted the strong connection between the SSN and issues of privacy. *Id*. at 779. He cited an FTC interpretation from 1973 that deemed selling lists of individual credit ratings as violations of the Fair Credit Reporting Act, since they invaded consumers' privacy. *Id*. at 779-80. The FTC opinion continued by saying that though publication of these ratings by name was an invasion of privacy, it would not be an invasion to publish the ratings by SSN. *Id*. at 780. Senator Percy strenuously disagreed with this assessment, noting that the SSN was "widely accessible." *Id*. at 780.

Senator Goldwater later introduced the amendment to S.3418 for consideration. *Id*. at 804. He reiterated his concerns about both the dehumanizing aspects of an identification number, and, more importantly, the ability of government or business to track each person's past records:

> [O]nce we can be identified to the Administrator in government or in business by an exclusive number tied to each of our past activities—our travels, the kinds of library books we have checked out, the hotels we have stayed at, our education record, our magazine subscriptions, our health history, our credit and check transactions—we can be pinpointed wherever we are. We can be manipulated. We can be conditioned. And we can be coerced.

Id. at 805. Senator Percy commented on the increasing computerization of data and records, and how the SSN could become a key to "the indexing and identification of individuals." *Id.* at 807. The amendment was accepted. *Id.*

That same day (November 21), the House considered and accepted a parallel amendment to H.R. 16373. Offered by Representative Goldwater, Jr., the amendment also restored to the bill language excised in committee. *Id.* at 932-33. Like the Senate amendment, it prohibited agencies from denying rights, benefits, or privileges based on an individual's refusal to disclose their SSN. *Id.* at 932. It also did not apply to any systems of records operating prior to 1975. *Id*. However, the House amendment covered only government agencies acting in compliance with federal law or under a federally assisted program, and still allowed the use of the SSN for verification. *Id*. Representative Goldwater

noted the objections to the moratorium on SSN use in the original bill—that altering existing systems based on the SSN would be chaotic and costly—and said that this would not be a problem with the proffered amendment because of its grandfather clause. *Id*. at 933. The amendment to the House bill was accepted. *Id*. at 935.

The differences between the House and Senate versions were resolved informally in a series of compromise amendments that eliminated the authentication exception from the House version and broadened its scope to match the Senate's version, which precluded all government agencies from creating new systems using the SSN. *Id*. at 864. The Senate provision for informing individuals of the nature, authority, and purpose of the request was also included. *Id*. These changes were accepted by the Senate on December 17, and by the House on December 18. *Id*. at 838, 893. The limitations on the use of the SSN were enacted as §7 of the Privacy Act. Pub. L. 93-579, §7.

C. The OMB Guidelines of 1975

In 1975, the OMB issued authoritative regulations for agencies implementing the Privacy Act, pursuant to section 6 of the Privacy Act that also gives the OMB continuing powers to oversee agencies' implementation of the Act. Pub. L. 93-579, §6. Office of Management and Budget, Guidelines for Implementing Section 552a of Title 5 of the United States Code, (1975) ("OMB Guidelines"), reprinted in Legislative History at 1015. Among other things, the OMB Guidelines explicate the civil remedies available to plaintiffs under the Privacy Act. OMB Guidelines at 71.

The OMB Guidelines enumerate three requirements for an individual to sue under subsection (g)(1)(D): the action was "intentional or willful"; the agency's action had an

"adverse effect" upon the individual; and the "adverse effect" was causally related to the agency's actions. *Id*. at 74. Once these criteria are met, the OMB requires no additional showing:

> When the court finds that an agency has acted willfully or intentionally in violation of the Act in such a manner as to have an adverse effect upon the individual, the United States will be required to pay
>
> —actual damages or $1,000, which ever is greater
>
> —court costs and attorney fees.

Id. at 77. This excerpt also indicates the OMB's interpretation of the phrase contained in the Act "but in no case shall a person entitled to recovery receive less than the sum of $1,000." 5 U.S.C. § 552(g)(1)(D), By providing that a plaintiff should receive the greater of actual damages or $1,000 without any additional showing, the OMB Guidelines confirm that a successful plaintiff is entitled to $1,000 as statutory damages.

Congress explicitly delegated to the OMB the task of developing guidelines for the application of the Privacy Act. 5 U.S.C. § 552a(v). The OMB Guidelines clearly provide for statutory damages of $1,000. OMB Guidelines at 77. Since the OMB Guidelines are a reasonable interpretation of a statute that the OMB was charged with overseeing, the court should defer to the agency's interpretation of the statute. *Chevron U.S.A., Inc. v. NRDC*, 467 U.S. 837 (1984).

CONCLUSION

The willful and intentional disclosure of Social Security Numbers constitutes a substantial invasion of

privacy, as Congress and the courts have recognized. Congress created a liquidated damages provision in the Privacy Act to discourage wrongful disclosures of the SSN. This interpretation is based on the landmark report that provided the basis for the Act, the legislative history of the Act, and the OMB Guidelines that followed the Act.

At a time when identity theft, facilitated by the misuse of the SSN, is on the rise, the Court should ensure that this critical purpose in the Privacy Act is not lost. Requiring high thresholds of proof of actual damages for SSN misuse would undermine public safety and the very purpose of the Act.

Dated: August 25, 2003

Respectfully submitted,

MARC ROTENBERG
Counsel of Record
DAVID L. SOBEL
CHRIS JAY HOOFNAGLE
MARCIA HOFMANN *
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140
*: Admission pending in the District of Columbia