IN THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

No. 09-1723

BETTY J. OSTERGREN

Plaintiffs-Appellee/Cross-Appellant,

vs.

ROBERT F. McDONNELL

Defendants-Appellant/Cross-Appellee.

AMICUS CURIAE BRIEF OF ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PLAINTIFFS AND APPELLEES AND URGING AFFIRMANCE

On Appeal from the United States District Court for the Eastern District of Virginia

---

BRIEF FOR EPIC AND TECHNICAL EXPERTS AND PRIVACY SCHOLARS

MARC ROTENBERG
Counsel of Record
JOHN VERDI
JARED KAPROVE
MATTHEW PHILLIPS
Electronic Privacy Information Center
1718 Connecticut Ave., NW Suite 200
Washington, DC 20009
(202) 483-1140

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c)
for Case No. 09-1723

Amicus Curiae, Electronic Privacy Information Center ("EPIC"), is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of the stock of EPIC.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICUS CURIAE*[1]

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values. EPIC has participated as *amicus curiae* in several cases before the U.S. Supreme Court and other courts concerning emerging privacy issues, new technologies, and Constitutional interests, including *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009) *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *National Cable and Telecommunications Association v. Federal Communications Commission*, 555 F.3d 996 (D.C. Cir. 2009); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006) 470 F.3d 1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003).

---

[1] All parties have consented to the filing of this brief. Fed. R. App. P. 29(a).

EPIC has a particular interest in protections that limit disclosure of Social Security Numbers (SSNs). EPIC has filed several *amicus* briefs in federal and state courts concerning the specific risks to privacy that result from the unnecessary and improper collection of the SSN. *Doe v. Chao*, 540 U.S. 614 (2004) (damage award in cases concerning the unlawful disclosure of the SSN under Privacy Act); *Ingerman v. Internal Revenue Service*, 953 F.2d 1380 (3d Cir. 1991) (SSN displayed publicly in correspondence from the IRS); *Griedinger v. Davis*, 988 F.2d 1344 (4th Cir. 1992) (SSN published in the voting rolls); and *Beacon Journal Publishing v. City of Akron*, 70 Ohio St. 3d 605 (Ohio 1994) (SSN available in public records). Several members of the EPIC Advisory Board are leading experts in the development of security protocols, data collection practices, and other related technical measures that seek to minimize the risks of identity theft and fraud.

Amici Technical Experts and Legal Scholars

Grayson Barber

Christine L. Borgman,
Professor & Presidential Chair in Information Studies, UCLA

Dr. Whitfield Diffie, Dr. sc. techn. (hc), ScD (hc)

Deborah Hurley

Pradeep K. Khosla,
Dean, Carnegie Mellon University College of Engineering and Dowd University Professor

Pablo Molina,
Associate VP of IT and Campus CIO, Georgetown University

Helen Nissenbaum,
Professor of Media, Culture & Communication, NYU

Peter G. Neumann,
Principal Scientist, SRI International Computer Science Lab

Deborah C. Peel, M.D.,
Founder, Patient Privacy Rights

Bruce Schneier,
Security Technologist

Robert Ellis Smith,
Publisher, Privacy Journal

Dr. Latanya Sweeney, Ph.D.
Distinguished Career Professor, Carnegie Mellon University, School of Computer Science, Institute for Software Research.
Visting Professor, Harvard University, Computer Science, Center for Research on Computation and Society.
Visting Professor, Massachusetts Institute of Technology (MIT), Computer Science and Artificial Intelligence Lab (CSAIL)

SUMMARY OF THE ARGUMENT

The basic right of personal privacy has long been recognized and protected in our legal system, and the particular risk that the unregulated use of the Social Number (SSN) poses to this right has been a matter of substantial interest by courts and legislatures. Accordingly, the collection and dissemination of the SSN has been tightly restricted. Congress addressed the privacy risks associated with SSN disclosure through the Privacy Act of 1974, and many states, including Virginia, have since passed laws to limit the use of the SSN in the private sector. Nonetheless, the unnecessary use of the Social Security Number has drastically expanded. Identity theft is a problem affecting millions of people and inflicting losses in the billions, in addition to non-monetary losses. Both public and private databases, containing SSNs, have been subject to breach and theft. It is clear that more needs to be done to protect the privacy of the SSN.

Ostergren's advocacy work focuses on reducing identity theft arising from the improper disclosure and dissemination of the Social Security Number. Virginia makes available unredacted Social Security Numbers to the public through documents hosted on its remote-access, Internet-based system. Anyone anywhere in the world with access to a computer is able to find these web sites, maintained by Virginia, and download these documents containing the SSNs of Virginia state residents.

Ostergren raises awareness of the identity theft problem by extracting the Social Security Numbers of certain public officials from those publicly available documents and republishing them on her website. She obtains no commercial value from the publication of the SSNs, nor does she obtain the SSNs so that anyone else may obtain commercial value or cause harm. He activity is pure speech, intended to call attention to the precise problem of SSN availability by publishing the SSNs of the relevant Virginia state officials who make the SSNs available.

The Supreme Court has consistently held that, when a person lawfully obtains truthful information that implicates a matter of public significance and publishes that information, the publication is protected by the First Amendment, and punishment may be imposed, if at all, only when narrowly tailored to a state interest of the highest order. Ostergren lawfully obtained from the government the Social Security Numbers that she republished. Her speech advocating increased awareness of identity theft and improved privacy protection implicates a matter of substantial public significance. Finally, the punishment is not narrowly tailored to a state interest of the highest order because there are several less restrictive alternatives and, significantly, because Ostergren's speech in fact advances the state's ostensible interest in reducing identity theft.

Protecting Ms. Ostergren's constitutional right to free speech will not unduly interfere with the Commonwealth's ability to protect its citizens' privacy against

data mining and disclosure by commercial interests because commercial speech is governed by intermediate scrutiny, a lower standard. As such, we urge the court to affirm the decision of the court below and find that the Virginia statute is unconstitutional as applied to Ms. Ostergren.

ARGUMENT

I. The Unnecessary Disclosure of SSNs Creates Substantial Privacy Risks

A. The Regulation of the SSN

The SSN was established in 1936 as a nine-digit account number "to facilitate the early manual bookkeeping operations associated with the creation of Social Security in the 1930s." Social Security Administration, Frequently Asked Questions, Q18[2]. 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 June 15, 1937)[3]. 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 Security 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[4].

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

---

[2] *Available at* http://www.ssa.gov/history/hfaq.html
[3] *Available at* http://www.ssa.gov/history/reg1.html.
[4] *Available at* http://www.ssa.gov/history/hfaq.html

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, as evidenced by the series of hearings in the 1960's 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.

Two years later, an HEW advisory committee issued a report recommending the development of extensive legal safeguards for the record systems maintained by the federal government. *HEW Report* at 121. The advisory committee warned that the use of the SSN as a personal identifier "would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems . . ." *Id.* at

122 (footnote omitted). In recognition of that risk, the advisory committee recommended the enactment of restrictions on the disclosure and dissemination of the SSN. The *HEW Report* recommended that:

- Uses of the Social Security Number be limited to only those purposes required by the federal government.
- Federal agencies should not require the use of the Social Security Number absent statutory authority.
- Congress evaluate any proposed use of the Social Security Number
- Individuals have the right to refuse to provide their Social Security Numbers, and should suffer no harm for exercising this right.
- Organizations required by Federal law to obtain the Social Security Number use the number solely for the purpose for which it was obtained and not make any secondary use or disclose the Number without the informed consent of the individual.

Id. at 124-25.

Congress adopted those recommendations the following year through passage of the Privacy Act, P.L. 93-579, 88 Stat. 1896 (1974). *See* S. Rep.No. 1183, 93d Cong., 2d Sess. reprinted in 1974 U.S. Code Cong. and Admin. News 6916, 6944-46 (citing *HEW Report*).

The Privacy Act makes clear that Congress gave special recognition to the need to control the misuse of the SSN. Section 7 makes it unlawful for any agency to deny any right, benefit or privilege to any individual "because of such individual's refusal to disclose his social security account number." It further

provides that any agency requesting an individual to disclose his or her SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." P.L. 93-579, Sec. 7, 88 Stat. 1896, 1909 (1974), reprinted in 5 U.S.C. § 552a note (1982).

In Section 3 of the Act, Congress provided that

> [n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be [in compliance with several specified exceptions not applicable here].

5 U.S.C. § 552a(b). In enacting these protections, Congress sought to curtail the privacy violations made possible by the proliferation of the SSN.

> Citizens' complaints to Congress and the findings of several expert study groups have illustrated a common belief that a threat to individual privacy and confidentiality of information is posed by [expanding use of the SSN]. The concern goes both to the development of one common number to label a person throughout society and to the fact that the symbol most in demand is the Social Security number, the key to one government dossier.
> * * *
> A cross-section of such complaints appearing in the subcommittee hearings shows that people are pressured in the private sector to surrender their numbers in order to get telephones, to check out books in university libraries, to get checks cashed, to vote, to obtain drivers' licenses, to be considered for bank loans, and many other benefits,

rights or privileges.

S. Rep. No. 1183, 93d Cong., 2d Sess., *reprinted in* 1974 U.S. Code Cong. and Admin. News 6916, 6944.

The SSN privacy concerns Congress addressed in 1974 have even greater force today. Technological advancements and the computerization of public and private sector databases have hastened the trend toward unnecessary reliance on the SSN.

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. U.S. Gen. Accounting Office, *Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* 8 (2009) [hereinafter "*GAO ID Theft Report*"]. The GAO has recognized the risk of identity theft via SSN disclosure, calling SSNs a "critical piece of information used to perpetrate identity theft." *Id.* at 8. SSNs are highly sought by identity thieves, and "often are described as the 'keys to the kingdom,' because an identity thief with a consumer's SSN (and perhaps other identifying information) may be able to use that information to . . . open new accounts, access existing accounts, or obtain other benefits in the consumer's name." Fed. Trade

Comm'n, *Security in Numbers: SSNs and ID Theft* 2 (2008).

Identity theft victimizes millions of people each year. The FTC estimated that 8.3 million people discovered that they were victims of identity theft in 2005, with total reported losses exceeding $15 billion. Fed. Trade Comm'n, 2006 *Identity Theft Survey Report* 4, 9 (2007) [hereinafter "*FTC ID Theft Report*"]. The GAO has identified numerous examples of public and private databases that were compromised and SSNs that were stolen. *GAO ID Theft Report* at 3-4, 11-12. In a recent report on the issue, the GAO reiterated that, "[w]ithout proper safeguards in place, SSNs will remain vulnerable to misuse, thus adding to the growing number of identity theft victims." U.S. Gen. Accounting Office, *Social Security Numbers: More Could Be Done to Protect SSNs* 17 (2006).

Peter Neumann, an expert on privacy and security (and a member of the EPIC Advisory Board), testified to Congress in 2007 about security and privacy, and concluded that the design of information systems are subject to many pitfalls, and that there is "[a] common tendency to place excessive faith in the infallibility of identification, authentication, and access controls to ensure security and privacy." *Security and Privacy in the Employment Eligibility Verification System (EEVS) and Related Systems: Hearing Before the H. Comm. On Ways and Means Subcomm. On Social Security*, 110th Cong. 9 (2007) (statement of Peter G.

Neumann, Principal Scientist, Computer Science Lab, SRI International).[5]

The excessive faith placed in systems safeguarding SSNs has been unfounded, as demonstrated by several recent examples of data breaches that have compromised SSNs. On August 5, 2009, a prison inmate obtained the SSNs of approximately 1,000 state employees in New Hampshire. Lauren Collins, *Inmate Found With Social Security Information at NH Prison*, New England Cable News, Aug. 5, 2009.[6] Since 2006, data about almost 30 million active and retired service members has been stolen from four Veteran's Affairs offices. Byron Acohido & Jon Swartz, *Military Personnel Prime Targets for ID Theft*, USA Today, June 15, 2007.[7] In EPIC's testimony to the House Committee on Ways and Means' Subcommittee on Social Security, Marc Rotenberg noted social security number data breaches that occurred within the states of each member of the subcommittee. *Protecting the Privacy of the Social Security Number from Identity Theft: Hearing Before the H. Comm. on Ways and Means Subcomm. On Social Security*, 110th Cong. (2007) (statement of Marc Rotenberg, President, EPIC).[8]

After data breaches occur, many of the problems that result from the misuse

---

[5] *Available at* http://www.acm.org/usacm/PDF/EEVS_Testimony_Peter_Neumann_USACM.pdf.
[6] Available at http://www.necn.com/Boston/New-England/2009/08/05/Inmate-found-with-Social/1249503276.html.
[7] *Available at* http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-06-14-military-id-thefts_N.htm?csp=34
[8] *Available at* http://www.epic.org/privacy/ssn/idtheft_test_062107.pdf

of the SSN are also not purely financial. Data collected by the Federal Trade Commission highlight the non-monetary losses suffered by individuals whose identities have been stolen. *FTC ID Theft Report* at 7. Roughly 37% of victims reported non-monetary harms as defined by the FTC. *Id.* Non-monetary harms that were discussed were denial of credit; inability to use credit cards; inability to obtain loans; having utilities cut off; harassment by debt collectors; being subjected to criminal investigation, arrest, or conviction; having a civil suit filed or judgment entered against them; and having difficulty obtaining or accessing existing bank accounts. *Id.*

C. Businesses Continue to Sell SSNs, Placing the Privacy of Americans at Risk

The private sector's use of SSNs has continued to grow. Not only has the number continued to be used as an identifier in a number of contexts, as described in the 1974 Congressional report, but an entire industry has sprung up around the processing and sale of Americans' personal information. These data aggregation companies, also known as data miners and data brokers, have compiled extensive databases from public sources containing huge amounts of information on American citizens, including credit information and SSNs. They then sell this information to purchasers on both large and small scales, making it increasingly difficult for people to maintain control over their own information.

Some of the world's biggest data brokers are the companies Choicepoint,

Acxiom, and Equifax. ChoicePoint was purchased by LexisNexis parent company Reed Elsevier in 2008 for over $4 billlion. Ellen Nakashima & Robert O'Harrow Jr., *LexisNexis Parent Set to Buy ChoicePoint*, Wash. Post, Feb. 22, 2008.[9] As LexisNexis already maintained considerable databases of its own, the merged companies' stores of information are now even more substantial. *Id.*

A major risk of these large databases of personal information is the risk that the security will be breached in some way and the information will fall into the hands of unauthorized users. This can happen a number of different ways, including computer hacking, physical theft, dishonest employees, and even by accident, through something as simple as an employee leaving a laptop bearing sensitive data in an airport. For an extensive and regularly updated list of reported data breaches in the United States, *see* Privacy Rights Clearinghouse, *A Chronology of Data Breaches*.[10] Just as large of a risk, however, is when apparently authorized users obtain data from data brokers for nefarious purposes. In 2005, ChoicePoint announced that identity thieves had posed "as officials in legitimate debt collection, insurance, and check-cashing businesses" and purchased dossiers on well over 100,000 Americans. Robert O'Harrow, Jr., *ID Data Conned*

---

[9] *Available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/02/21/AR2008022100809.html.
[10] http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP.

From Firm, Wash. Post, Feb. 17, 2005;[11] *see also* EPIC, ChoicePoint (last visited Oct. 15, 2009).[12] As long as companies like ChoicePoint continue to get access to personal information, including SSNs, from public records, these risks will continue.

D. States Have Adopted New Laws to Safeguard SSNs

In response to the identity theft threat, several states have adopted laws restricting the use and disclosure of SSNs. California, for example has enacted several laws protecting SSNs since 2001. One statute places important restrictions on use of the SSN, prohibiting companies and people from publicly posting an SSN, and prohibiting the printing of an SSN on an identity card or document used to obtain a product or service. *See* Cal. Civ. Code § 1798.85 (West. Supp. 2009). Businesses that use the SSN to identify customers, such as utility companies, are not permitted to print the SSN on invoices or bills sent through the mail. *Id.* The transmission of SSNs on the Internet is prohibited unless the connection is secure or the number is encrypted. *Id.* Another statute grants individuals the ability to request that a "security alert" be placed on their credit record, and enables Californians to request a "security freeze" that prevents credit agencies from releasing personal information from an individual's credit report. Cal. Civ. Code § 1785.11.2 (West Supp. 2009). California law also requires companies that maintain

[11] *Available at* http://www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html.

SSNs and other personal information to notify individuals of security breaches. Cal. Civ. Code §§ 1798.29, 1798.82 (West Supp. 2009).

Subsequently, 13 other states—Arizona, Arkansas, Connecticut, Georgia, Illinois, Maryland, Michigan, Minnesota, Missouri, Oklahoma, Texas, Utah, and Virginia—enacted laws similar to California's, according to a 2007 GAO report. *See* U.S. Gen. Accounting Office, *Social Security Numbers: Use Is Widespread and Protection Could Be Improved 4* (2007). According to a February 2009 journal article, "[f]orty-four states now have some form of a security breach notice law. . . . Forty-seven states and the District of Columbia have credit freeze laws. . . . [And] thirty-three states have some form of a Social Security number protection law." Patricia Covington & Meghan Musselman, *Privacy and Data Security Developments Affecting Consumer Finance in 2008*, 64 Bus. Law. 533, n.20, n.44, n.61 (2009).

Colorado is one example of a state with laws protecting SSNs. A 2004 Colorado law imposes statutory restrictions on the collection and use of SSNs. Colo. Rev. Stat. § 6-1-715 (2009). It limits the collection of the SSN and its incorporation in licenses, permits, passes, or certificates issued by the state. *Id.* The Colorado law also requires the establishment of policies for safe destruction of documents containing the SSN. *Id.* Insurance companies operating in the state must

---

[12] Available at http://epic.org/privacy/choicepoint/

remove the SSN from consumers' identification cards. *Id.* Finally, the legislation creates new penalties for individuals who use others' personal information to injure or defraud another person. *Id.*

More recently, New York enacted a law, effective January 1, 2008, that closely resembles California law and places limits on the use and dissemination of SSNs. *See* N.Y. Gen. Bus. Law § 399-dd (2009). Applicable to all nongovernmental bodies, the law makes it illegal to intentionally communicate another person's SSN to the general public. *Id.* The law also prohibits anyone from requiring identity cards displaying SSNs before providing access to services, benefits or products. *Id.* As in the California law, the New York law requires Internet transmission of SSNs to be either over a secure connection or encrypted. *Id.* Finally, the law prohibits the use of SSNs in mail correspondence, with certain exceptions. *Id.*

Finally, Virginia law also restricts the use and dissemination of SSNs. *See* Va. Code Ann. § 59.1-443.2 (2009). In the provision at issue in this case, Virginia law provides that "[e]xcept as otherwise specifically provided by law, a person shall not . . . [i]ntentionally communicate another individual's social security number to the general public." *Id.* at § 59.1-443.2(A)(1). The statute also prohibits printing SSNs on identification cards, requiring the use of SSNs to access websites (unless another authentication device is also required), or sending mail on which an

SSN is visible. Id. at § 59.1-443.2(A)(2)-(4).

It is important to recognize that these state statutes, limiting the use of the SSN, address a wide variety of concerns, from identity theft to commercial exploitation to poorly conceived security practices. But none of them are intended to limit the speech of a privacy advocate who seeks to draw attention to the risks associated with the availability of SSNs. Indeed, it is quite possible that some of these new SSN privacy laws came about in part because of the concerns raised by Ostergren.

E. Research Has Demonstrated That Certain Techniques to Obscure SSNs Do Not Solve the Privacy Problem

Despite some states' attempts to safeguard SSNs through technical means, the privacy risks associated with the disclosure of SSNs are not eliminated even if only the final four digits of an individual's SSN are disclosed, as identity thieves may be able to reconstruct the full SSN from the truncated digits. Thus, although the states' efforts are encouraging, more robust protection is needed to truly safeguard SSNs.

Quasi-identifiers can be used for re-identification because they can be linked to external databases that contain identifying variables. This method, record linkage, occurs when two or more databases are joined. Such information can be obtained through public records, such as birth and death certificates. *See* Salvador Ochoa et al., *Re-identification of Individuals in Chicago's Homicide Database: A*

Technical and Legal Study, Massachusetts Institute of Technology (2001) (utilizing the Social Security Death Index and de-identified information about Chicago homicide victims, the researchers were able to re-identify 35% of the victims). Using record linkage, de-identified data can also be easily re-identified. For example, by utilizing date of birth, gender, and zip code information for members of the public, a researcher was able to uniquely identify 87% of the US population. Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality*, 25 J. Law, Med., & Ethics 98, 98–99 (1997).

Similarly, according to the GAO, complete SSNs may be reconstructed from truncated digits by simply comparing truncated SSNs in federally generated public records, which provide only the final four digits, to truncated SSNs provided by many information resellers, which provide only the first five digits. U.S. Gen. Accounting Office, *Identity Fraud Survey Report: Consumer Version* 2-3 (2009). Thus, by simply comparing the two records, a complete SSN can be reconstructed. *Id.* at 3.

Moreover, in a study published in July 2009, two researchers at Carnegie Mellon University found that an individual's entire SSN often could be predicted from publicly available birth information. *See* Alessandro Acquisiti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 Proceedings of the National Academy of Sciences 10975 [hereinafter "*SSN Study*". Moreover, the

first five digits of an individual's SSN could be predicted with an even greater degree of accuracy. The accuracy of the researchers' predictions was even greater when predicting the numbers of individuals born in sparsely-populated states like Montana, and the researchers anticipate that their predictions will become increasingly accurate over time.

SSNs are predictable largely because they are not truly random, and the federal government has disclosed the method by which SSNs are assigned. *See* Social Security Administration, SSN - Order of Issuance.[13] The first three digits of an SSN are its area number (AN), the next two are its group number (GN), and the last four are its serial number (SN). *See id.* ANs are assigned based on the zipcode of the mailing address provided in the application for a SSN. *See* Social Security Administration, Social Security Number Allocations.[14] GNs are assigned in a pre-determined but nonconsecutive order between 01 and 99. *See* Social Security Administration, SSN - Order of Issuance.[15] The ANs assigned to each state and the sequence of GNs are publicly available. *See* Social Security Administration, Social Security Number Allocations.[16] Finally, SNs are assigned consecutively from 0001 through 9999. *See* Social Security Administration, SSN - Order of

---

[13] Available at http://www.socialsecurity.gov/employer/ssnweb.htm.
[14] *Available at* http://www.socialsecurity.gov/employer/stateweb.htm.
[15] *Available at* http://www.socialsecurity.gov/employer/ssnweb.htm.
[16] *Available at* http://www.socialsecurity.gov/employer/stateweb.htm.

Issuance.[17]

Given that predictability, the researchers discovered that they could determine an individual's SSN by comparing the individual's birth information to the birth information of deceased individuals, which is publicly available in the Social Security Administration's (SSA) Death Master File (DMF). *See SSN Study* at 10975. The DMF contains the SSNs of individuals whose deaths have been reported to the SSA.

Using that method, the researchers were able to predict, in only one attempt, the first five digits for 7% of individuals born nationwide between 1973 and 1988, and 44% for individuals born after 1988. *Id.* at 10977. Moreover, in fewer than 1,000 attempts they were able to determine the complete SSN for 0.8% of individuals born between 1973 and 1988, and 8.5% of those born after 1988. *Id.* at 10978. Finally, the accuracy of their complete-SSN predictions increased by more than 60% if the individual was born recently and in a less populous state. *Id.*

Thus, the researchers concluded that limiting the disclosure of Social Security Numbers to only the last four digits was insufficient to eliminate privacy risks: "the first [five] digits of an SSN are those, in fact, easier to infer. This leaves even redacted or truncated SSNs still predictable—and, therefore, still vulnerable." *SSN Study* at 10980. Thus, even if states have taken steps to protect SSNs through

---

[17] *Available at* http://www.socialsecurity.gov/employer/ssnweb.htm.

technical methods, this does not ensure that SSNs are not eventually disclosed. Further advocacy on this point could lead to more robust solutions to the SSN problem.

II. Because of the Threat of Identity Theft Created by SSN Disclosure, Ostergren's Advocacy Is Protected Speech Under the First Amendment, But Similar Speech by Commercial Interests Is Not

Identity theft is a serious problem, and Virginia has a correspondingly strong interest in regulating the disclosure of SSNs in order to prevent the theft of its citizens' identities. At the same time, Ostergren's advocacy is protected speech that helps advance the interest of the state's residents. Her speech is specifically intended to express a political viewpoint about the failure of the state to fulfill its purpose. If the state is permitted to silence her, the problem of identity theft would receive less attention. In contrast, the collection and dissemination of vast numbers of SSNs for commercial gain, such as by a data-mining or data broker company, would not be protected, as it would not speak to a matter of public concern, and would seek only to commoditize the information.

A. The First Amendment Protects the Right to Publish Information in Government Records, Particularly When Speaking on a Matter of Public Significance

1. The Supreme Court Has Universally Held That the First Amendment Shields the Publication of Information in Government Records When Speaking on a Matter of Public Concern

The Supreme Court has repeatedly held that "state action to punish the publication of truthful information seldom can satisfy constitutional standards," and that "a penal sanction for publishing lawfully obtained, truthful information . . . requires the highest form of state interest to sustain its validity." *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97, 101-02 (1979). Moreover, our legal system has long recognized that "[t]he right of privacy does not prohibit any publication of matter which is of public or general interest." Samuel Warren & Louis Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193, 214 (1890); *Bartnicki v. Vopper*, 532 U.S. 514, 534 (2001) ("privacy concerns give way when balanced against the interest in publishing matters of public importance"). Indeed, if the publication is "about a matter of public significance, then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order." *Daily Mail* at 103; *Bartnicki* at 527-28. The basic principle guiding the First Amendment's protection of speech on matters of public significance is our "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open." *New York Times Co. v. Sullivan*, 376 U.S.

254, 270 (1964).

Applying those rules, the Supreme Court has consistently shielded free speech and refused to permit the government to sanction the publication of truthful information obtained from the government when the speech concerns a matter of public significance. For instance, in *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), the Court held that the First Amendment prevented the state from punishing a television station for publishing the name of a deceased rape victim that was obtained from open court records. 420 U.S. at 496-97. Although the Court did not hold that *any* truthful publication was constitutionally protected, it held that "[a]t the very least, the First and Fourteenth Amendments will not allow exposing the press to liability for truthfully publishing information released to the public in official court records." *Id.* at 496. Similarly, the Court in *Daily Mail* held that even if the government does not itself provide access to the information, "[i]f the information is lawfully obtained . . . the state may not punish its publication except where necessary" to further a state interest of the highest order. 443 U.S. at 104. In *Daily Mail*, the state's interest in protecting the anonymity of a juvenile offender was insufficient.

In *The Florida Star v. B.J.F.*, 491 U.S. 524 (1989), the Court further clarified the rationale behind *Cox* and *Daily Mail*, reaffirming the rules articulated in those cases based on the "overarching 'public interest, secured by the

Constitution, in the dissemination of truth," and three other considerations. *Id.* at 534 (quoting *Cox*, 420 U.S. at 491). First, the Court noted that where information is lawfully obtained, the "government retains ample means of safeguarding significant interests upon which publication may impinge. . . . Where information is entrusted to the government, a less drastic means than punishing truthful publication almost always exists for guarding against the dissemination of private facts." *Id.* at 534. Second, the Court found that:

> punishing the press for its dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act. . . . [W]here the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release.

Id. at 535. Finally, the Court noted that "'timidity and self-censorship' may result from allowing the media to be punished for publishing certain truthful information,'" a problem that *Cox* recognized in the context of "information made public through official court records." *Id.* (quoting *Cox*, 420 U.S. at 496).

The *Florida Star* court also clarified that a "matter of public significance," is one where "the article generally, as opposed to the specific identity contained within it, involved a matter of paramount public import." *Id.* at 536-37. That case involved a matter of public significance where a newspaper reported on a robbery and sexual assault that had been reported to the authorities. *Id.* at 537.

Finally, the *Florida Star* court held that the statute imposing liability on the

newspaper for publishing the victim's name did not serve a state interest of the highest order, despite the state's interests in "the privacy of victims of sexual offenses; the physical safety of such victims . . . ; and the goal of encouraging" the reporting of sexual offenses. *Id.* at 537. The state interest was insufficient for three independent reasons: (1) "where the government itself provides the information, [it presumably has] far more limited means of guarding against dissemination than the extreme step of punishing truthful speech"; (2) the statute imposed per se liability without "individualized adjudication"; and, (3) the "facial underinclusiveness" of the statute, which only punished dissemination by "instruments of mass communication." *Id.* at 538-40.

Most recently, in *Bartnicki*, the Court reemphasized that the "core purposes of the First Amendment" are implicated when the state "imposes sanctions on the publication of truthful information of public concern." 532 U.S. at 533-34. Under that principle, the Court concluded that speech was of public significance where a newspaper used information that was illegally obtained by a third party when reporting on negotiations over teacher salaries. The negotiations were "unquestionably a matter of public concern, and [the newspaper was] clearly engaged in debate about that concern."

2. Ostergren's Speech is Protected Under the First Amendment

Ostergren's speech closely resembles the speech at issue in the *Daily Mail* line of cases, and it should be shielded by the First Amendment for the same reasons. Under the definition articulated in *Florida Star*, Ostergren's speech concerns a matter of public significance because the general article—the privacy threat arising out of Virginia's failure to prevent the publication of SSNs—rather than the individual identity of the SSNs she disclosed, involve a matter of paramount public import. *See supra* Part I.B. Indeed, Ostergren's advocacy is at the apex of protected speech under that line of cases. It serves no commercial interest, does not seek to commoditize the SSN information, and is engaged directly in the debate about the issue of public concern—privacy and identity theft.

Moreover, the suppression of Ostergren's speech implicates many of the same concerns that animated the Court's decisions in those cases. Virginia has far less drastic means of guarding against the dissemination of SSNs. It could simply not publish the records online in the first place, or it could require records to be redacted before being published, or it could do a better job removing the SSNs before posting. In other words, it could try to solve the problem, instead of silencing a critic. Moreover, as the *Florida Star* court noted, it would be "highly anomalous" for Virginia to punish Ostergren, rather than the state actor itself, which was the initial publisher of the SSNs. Finally, to squelch Ostergren's speech

would cause advocates for government transparency and oversight to be timid and self-censoring on matters of grave public significance.

Even if the suppression of Ostergren's speech did not threaten the values at the core of the First Amendment, the state does not have an interest of the highest order that would justify such suppression. The same three independent considerations that led the *Florida Star* court to reject the state's interest as insufficient are present in this case. 491 U.S. at 537-40. First, as discussed, Virginia has far more limited means of guarding against dissemination. Second, the statute here imposes per se liability for disclosure, rather than conducting a case-by-case inquiry into the value of the speech. Finally, the statute here is facially underinclusive, as it does not sanction government employees who publish SSNs, thus demonstrating the government's lack of commitment to advancing its interest.

Moreover, even assuming that the statute serves a state interest of the highest order, it does not accomplish its stated purpose. In *Daily Mail*, the Court found that the "statute's approach [did] not satisfy constitutional requirements" where the statute only restricted the publication of juvenile offenders' information in newspapers, but not in other media, because the statute would not accomplish the stated purpose of protecting the juveniles' anonymity. 443 U.S. at 104-05. Similarly, the statute in this case does not accomplish the state's purported interest in preventing identity theft because it does not punish the disclosure of SSNs by

government actors, and because it does not distinguish between disclosures for the purpose of furthering identity theft and disclosures for the purpose of advocating for strengthened privacy rights.

B. Unlike Ostergren, Commercial Speakers Are Not Entitled to First Amendment Protection for Similar Speech

The doctrine discussed above does not prevent the Commonwealth of Virginia from protecting the privacy of its citizens SSNs against access and disclosure by data-mining companies and other commercial actors. Unlike the political speech practiced by Ms. Ostergren on her watchdog web site, commercial speech is governed by a different standard, set forth in *Central Hudson Gas & Elec. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980). *Central Hudson* establishes a four-part test for the regulation of commercial speech. First, for the speech to even be protected by the First Amendment, "it at least must concern lawful activity and not be misleading." *Id.* at 566. The second step is to determine whether the interest of the government in regulating the speech is substantial. *Id.* The final two steps of the analysis are to "determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest." *Id.* Under the *Central Hudson* test, the Virginia statute could still constitutionally target commercial data mining and disclosure.

The Court of Appeals for the District of Columbia Circuit, recently took up a

similar question in *Nat'l Cable & Telecomm. Ass'n v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) [hereinafter *NCTA*]. The court considered whether the FCC could constitutionally restrict telecommunications companies from sharing customer data with third parties without first obtaining customer consent through an "opt in" procedure. Using the *Central Hudson* test, the unanimous panel concluded that the Commission's consent requirement did not violate the petitioners' First Amendment rights.

The first part of the *Central Hudson* test varies slightly from the first part of the *Florida Star* test, in that it requires a higher standard: that the commercial speech not be misleading, as opposed to *Florida Star*'s "truthful" standard. This distinction is the first hint of variation in treatment for commercial speech. Regardless, it is possible to assume that personal information disclosed by data mining corporations would be truthful and not misleading.

The second step of the *Central Hudson* analysis is the primary place in which the standards differ. *NCTA*, 555 F.3d at 1001. While restrictions of noncommercial speech are held to a strict scrutiny standard, looking for the highest governmental interest, *Central Hudson* asks only that the government's interest be "substantial." *Central Hudson*, 447 U.S. at 566. The *NCTA* court found that it had "already held, in an analogous context, that 'protecting the privacy of consumer credit information' is a 'substantial' government interest, as *Central Hudson* uses

the term." *NCTA*, 555 F.3d at 1001 (quoting *Trans Union Corp. v. FTC*, 245 F.3d 809 (D.C. Cir. 2001)). In further support of the proposition that personal data privacy is a substantial government interest is the Supreme Court's language: "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *U.S. Dep't of Justice v. Reporters Comm'n for Freedom of Press*, 489 U.S. 749, 763 (1989).

The third and fourth steps of the *Central Hudson* test, that any restrictions "directly advance" the governmental interest, and that they be "not more extensive than is necessary to serve that interest" are also different from the strict scrutiny standard applied to noncommercial speech like that performed by Ms. Ostergren. In commercial speech intermediate scrutiny, this does not imply a least-restrictive-means test, nor does it require that the government show that it has chosen the best conceivable option, as it would for noncommercial content-based speech restrictions. *Bd. Of Trs. Of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 476–81 (1989). In fact the restriction need only be "in proportion to the interest served." *Id.* at 481 (quoting *In re R.M.J*, 455 U.S. 191, 203 (1982). Preventing commercial disclosure of citizens' social security numbers would certainly directly advance the government's goal of protecting its citizens' privacy, and it would do so in perfect proportion to the interest.

When applied to commercial speech, therefore, the statute would still

constitutionally further the Commonwealth's interest. As such, protecting Ms. Ostergren's First Amendment right to use the numbers as a method of political speech would not prevent the government from enforcing restrictions on other breaches of its citizens' information privacy.

CONCLUSION

Amicus Curiae respectfully request this Court to grant Appellee's motion to sustain the decision of the lower court.

Respectfully submitted,

Marc Rotenberg
John A. Verdi
Jared Kaprove
Matthew Phillips
Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

October 20, 2009

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 6,976 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word 2007 in 14 point Times New Roman style.

Dated: October 20, 2009

Marc Rotenberg
John A. Verdi
Jared Kaprove
Matthew Phillips
Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 20th day of October, 2009, this brief was electronically filed with the Clerk of Court using the CM/ECF system. Twenty-five copies of the foregoing Brief of *Amicus Curiae* were also filed with the Clerk of the Court by overnight delivery service, and two copies were shipped by commercial carrier for next-day delivery upon the following:

Stephen R. McCullough
Office of the Attorney General
900 E. Main Street
Richmond, Virginia 23219
smmcullough@oag.state.va.us

Rebecca K. Glenberg
American Civil Liberties Union of Virginia
Foundation, Inc.
530 E. Main Street, Suite 310
Richmond, Virginia 23219
(804) 644-8080

Dated: October 20, 2009

_____
Marc Rotenberg
John A. Verdi
Jared Kaprove
Matthew Phillips
Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140