**Record No. 09-1723**

**In the United States Court of Appeals**
**for the Fourth Circuit**

**BETTY J. OSTERGREN,**

*Plaintiff-Appellee,*

**v.**

**ROBERT F. McDONNELL**, in his official capacity as Attorney General of Virginia,

*Defendant-Appellant.*

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

# OPENING BRIEF

WILLIAM C. MIMS
Attorney General of Virginia

STEPHEN R. MCCULLOUGH
Virginia State Bar No. 41699
State Solicitor General
smccullough@oag.state.va.us
*Counsel of Record*

WILLIAM E. THRO
Special Counsel

September 8, 2009

MARTIN L. KENT
Chief Deputy Attorney General

STEPHEN M. HALL
Assistant Attorney General

OFFICE OF THE ATTORNEY GENERAL
900 East Main Street
Richmond, Virginia 23219

Telephone: (804) 786-2436
Facsimile: (804) 786-1991

*Counsel for Defendant/Appellant*

# TABLE OF CONTENTS

## TABLE OF CONTENTS - CONTINUED

Page

## TABLE OF CONTENTS - CONTINUED

# TABLE OF AUTHORITIES

Page

CASES

## TABLE OF AUTHORITIES - CONTINUED

Page



CONSTITUTIONAL PROVISIONS

## TABLE OF AUTHORITIES - CONTINUED

Page

STATUTES

## TABLE OF AUTHORITIES - CONTINUED

## TABLE OF AUTHORITIES - CONTINUED

Page

RULES



OTHER AUTHORITIES

## TABLE OF AUTHORITIES - CONTINUED

Page

## OPENING BRIEF

The Attorney General of Virginia submits this Opening Brief. For the reasons detailed below, the judgment should be reversed.

## INTRODUCTION

This case presents the problem of what one academic commentator calls "crime facilitating speech."[1] *Virginia Code* § 59.1-443.2(A)(1) provides that "a person shall not . . . [i]ntentionally communicate another individual's Social Security Number to the general public." The plaintiff displays Social Security numbers ("SSNs") on her website as part of her advocacy for greater protection from the risks associated with private information in government records. By displaying SSNs on her website, she exposes persons assigned these SSNs to a serious risk of identity theft. The danger is more than hypothetical. Criminals have, in fact, turned to Ostergren's website to obtain SSNs for criminal purposes. Although the First Amendment provides robust protections for all manner of speech, it does not go so far as to protect speech that exposes public officials or

[1] Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095 (2005).

members of the general public to the very real prospect of devastating criminal predation.

## STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION

The district court had subject matter jurisdiction under 28 U.S.C. § 1331, to entertain a complaint under 42 U.S.C. § 1983. This Court has appellate jurisdiction to review the final order of the district court under 28 U.S.C. § 1291 or, alternatively, 28 U.S.C. § 1292(a)(1).

The district court entered a permanent injunction on June 2, 2009, enjoining the application of *Virginia Code* § 59.1-443.2(A)(1), as applied to the plaintiff. J.A. 407. The Attorney General[2] noted his appeal on June 30, 2008. J.A. 408. The appeal is timely.

---

[2] Robert F. McDonnell has resigned as the Attorney General of Virginia. The current Attorney General is William C. Mims. Assuming this case is decided after mid-January, 2010, the new Attorney General should be substituted as the appropriate named party under Fed. R. App. P. 43(c)(2).

## STATEMENT OF THE ISSUE

When a person obtains the social security numbers of public officials from public records, can a State prohibit this person from disseminating these social security numbers on the internet in order to protect public officials from the devastating consequences of identity theft, as well as to prevent other violations of the law?

## STATEMENT OF THE CASE

*Virginia Code* § 59.1-443.2(A)(1) provides that "a person shall not . . . [i]ntentionally communicate another individual's social security number to the general public." Previously, the statute provided an exception for "records required by law to be open to the public." *Virginia Code* § 59.1-443.2(D)(ii) (2007). In 2008, the General Assembly removed this exception, making the prohibition on disseminating SSNs effective for persons who obtained the SSNs from public records. 2008 Va. Acts. ch. 820. Violation of the statute exposes the violator to civil sanctions, including fines, investigative demands, and injunctions. *Virginia Code* §§ 59.1-201 through 206. The statute is enforced through private actions, by local Commonwealth's Attorneys, or by the Attorney General. *Id.*

Before the 2008 change to the statute went into effect, Betty J. Ostergren filed a complaint in the United States District Court for the

Eastern District of Virginia. She alleged that the prohibition on disseminating SSNs that she gleaned from governmental records violates her First Amendment rights. J.A. 7. The plaintiff alleged that she posts SSNs that she has obtained from public records on her website as part of her political advocacy for greater privacy in public records. J.A. 9. The Attorney General agreed not to initiate any prosecution until the resolution of the plaintiff's complaint. J.A. 84.

On August 22, 2008, the district court, Judge Robert E. Payne presiding, declared *Virginia Code* § 59.1-443.2 unconstitutional "as to the plaintiff's website, www.TheVirginiaWatchdog.com as it existed on the date that this action was filed." J.A. 228. The court reasoned, first, that Ostergren obtained the records from a government source. J.A. 218. Second, the court observed that

> the SSN's in the court records are without doubt personal in nature and are entitled to privacy because they are the quintessential personal identifier; and SSNs are susceptible to misuse that can cause great harm, such as identity theft. Therefore, it should not be difficult for a court to conclude that the protection of SSNs from public disclosure should qualify as a State interest of the highest order.

J.A. 219. To determine whether an interest qualifies as one of the highest order, the court reasoned that "the State's view and conduct . . .

must supply the basis for such a conclusion." J.A. 219. In the district court's view, the fact that the State made certain records available online, and did not fully fund redaction of SSNs from these records, undercuts the notion that the "protection of SSNs is an interest of the highest order." J.A. 219. Finally, the court noted that the topic addressed by Ostergren's website is one of public significance. J.A. 222. Having enjoined the application of the statute to Ostergren's website, the district court further directed the parties to brief "the propriety and scope of injunctive relief." J.A. 228.

Following briefing by the parties, the district court on June 2, 2009, entered a permanent injunction. The court sought to "accommodate the First Amendment rights of Ostergren and, at the same time, afford[] some protection to innocent members of the public who have no control of the release of the public records containing their SSNs." J.A. 404. The court enjoined the "enforcement of Va. Code § 59.1-443.2 against any iteration of Ostergren's website, now or in the future, that simply republishes publicly obtainable documents containing unredacted SSNs of Virginia legislators, Virginia Executive Officers, or Clerks of Court." J.A. 406. However, Ostergren is

prohibited from posting documents containing the SSNs of other Virginia residents or citizens. J.A. 406.

## STATEMENT OF FACTS

### I. DISSEMINATION OF SOCIAL SECURITY NUMBERS CREATES A DANGER OF DEVASTATING IDENTITY THEFT.

SSNs are a nine-digit number assigned by the Secretary of Health and Human Services for the purpose of administering the SSNs. *See* 42 U.S.C. § 405(c)(2)(B). Initially, these numbers were to be used exclusively by the United States government as a means of tracking earnings to determine the amount of Social Security taxes to credit to each worker's account. Over time, however, SSNs came to be used by other government agencies as well as the private sector as a reliable means of identification.

As a consequence of widespread use, SSNs can be found in a variety of court records. For example, given the use of aliases by defendants in criminal cases, Virginia courts have used SSNs in criminal cases as a reliable identifier. The real estate industry has also made extensive use of SSNs. As a result, many documents filed in

Virginia courts in connection with real estate transactions contain SSNs. J.A. 378.

As this Court is well aware, enterprising criminals seized upon the widespread availability of SSNs to perpetrate a new and growing form of financial crime: identity theft. "[T]he SSN is highly sought by individuals seeking to create false identities for purposes such as fraudulently obtaining credit, violating immigration laws, or fleeing the criminal justice system." Statement of Barbara D. Bovbjerg, Social Security Numbers, Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain, United States Governmental Accountability Office, Testimony Before the Committee on Consumer Affairs and Protection and Committee on Governmental Operations, New York State Assembly 1 (September 15, 2005) ("Bovbjerg Statement").[3] An SSN, along with a birth date and a name, "are the three pieces of information most often sought by identity thieves." *Id.* at 3.

Once a person obtains a SSN, it becomes possible fraudulently to obtain credit cards, apply for public benefits, order checks and loot bank

---

[3] Available at: http://www.gao.gov/new.items/d051016t.pdf (last visited Sept. 8, 2009).

accounts. It can take years of determined effort, and considerable expense, to clean up the wreckage caused by identity theft. The district court noted that "the lives of victims of identity theft are severely altered for years after the theft occurs." J.A. 401. The average victim of identity theft suffers a loss of approximately $17,000, and will spend more than $1,000 and 600 hours of personal time dealing with the consequences of victimization. J.A. 401.

Furthermore, identity thieves are rarely caught and punished for their crimes. J.A. 401-02. Identity theft is no longer a rare phenomenon. J.A. 402. It has been described as the fastest-growing crime in the United States. J.A. 402. Losses associated with identity theft are estimated at over $50 billion per year. J.A. 402. *See also* Synovate, 2006 Identity Theft Survey Report prepared for the Federal Trade Commission (November 2007) (detailing statistics relating to the scope of the identity theft problem).[4]

[4] The survey report can be found at: www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (last visited Sept. 8, 2009).

## II. THE VIRGINIA GENERAL ASSEMBLY HAS TAKEN EXTENSIVE ACTION TO OBVIATE THE PROBLEMS ASSOCIATED WITH SSNS.

### A. The General Assembly has limited the use and disclosure of SSNs by state agencies, criminalized identity theft, and required disclosures when data breaches occur.

Virginia has taken extensive action to deal with the problems associated with the dissemination of SSNs. First, the General Assembly has limited the use of SSNs by state agencies.[5] Second, the General Assembly has criminalized identity theft. *Virginia Code* §

---

[5] *Virginia Code* § 2.2-3800 (prohibiting state agencies from displaying SSNs on mailings); *Virginia Code* § 2.2-3808 (prohibiting state agencies from displaying an entire SSN on state-issued identification cards); *Virginia Code* § 2.2-3808.1 (prohibiting state agencies from disclosing, among other things, SSNs); *Virginia Code* § 2.2-3815 (prohibiting disclosure of SSNs pursuant to Virginia Freedom of Information Act disclosures); *Virginia Code* § 17.1-227 (clerks of court "may refuse to accept any instrument submitted for recordation that includes a grantor's, grantee's or trustee's social security number" and that "the attorney or party who prepares the instrument has responsibility for ensuring that the social security number is removed from the instrument prior to the instrument being submitted for recordation."); *Virginia Code* § 20-121.03 (in divorce cases, no "pleading, motion, order, or decree . . . shall . . . contain the social security number of any party or of any minor child of a party"); *Virginia Code* § 24.2-444(C) (prohibiting the State Board of Elections and local registrars from maintaining a list of voters containing SSNs); *Virginia Code* § 24.2-1002.1 (making it a Class 5 felony to disclose or make an unauthorized use of a SSN of any applicant for voter registration); *Virginia Code* § 32.1-267 (limiting access to marriage certificates containing SSNs unless the SSNs are blocked from view).

18.2-186.3. Identity theft is Class 1 misdemeanor, and if the damage exceeds $200, the crime rises to a Class 6 felony. In connection with this crime, the General Assembly has established an "identity theft passport" program to assist those who have been victimized by identity theft. *Virginia Code* § 18.2-186.5. Third, if an entity experiences a breach of its security system, and, among other data, SSNs are taken, the entity must notify affected persons so that they may take protective measures. *Virginia Code* § 18.2-186.6.

B. Court records present a thorny problem that Virginia is addressing in a variety of ways.

Over a period of several decades, several hundred million documents with SSNs have accumulated in court records. J.A. 229. To address the problem prospectively, the General Assembly enacted a general statute prohibiting "any court clerk to disclose the social security number or other identification numbers appearing on driver's licenses." *Virginia Code* § 17.1-293(A). Beginning in 2004, clerks are prohibited from posting on the internet any document that contains, among other things, SSNs. *Virginia Code* § 17.1-293(B).

The law makes an exception for "secure remote access" of court records. *Virginia Code* § 17.1-293(E)(1). Secure remote access enables a

subscriber who signs and agreement and pays a fee to gain remote computer access to court records. J.A. 96, 378. *Virginia Code* §§ 17.1-279(D), 17.1-294. Although the General Assembly required clerks to redact SSNs from a record before making it available for secure remote access, this provision did not go into effect because it was contingent on a specific appropriation to pay for the redaction process, and the appropriation was not made. 2007 Acts. ch. 548, J.A. 197. The impetus for placing these records online was to facilitate real estate transactions. J.A. 196.

The statute mandating clerks to establish secure remote access to land records also requires circuit court clerks to comply with certain standards. *Virginia Code* § 17.1-294(A). The Virginia Information Technology Agency has established rules governing remote access to these records. These standards require persons wishing to have remote access to the records to provide the following information:

- last name
- first name
- business name
- street address
- City/State/Zip Code
- phone number
- Email address
- Citizenship status

- Signature

Security Standard for Remote Access to Court Documents, § 2.1.1, ITRM Standard SEC503-02, Effective March 28, 2005 (hereafter "Security Standard").[6] Furthermore, "[r]egistration must be in person or by means of a notarized or otherwise sworn application that establishes the prospective Subscriber's identity, business or residence address, and citizenship status." Security Standard § 2.1.2. Each individual user or employee must obtain a password from the clerk. Security Standard § 1.4(3). If an employee with remote access is terminated, the subscriber must immediately notify the clerk's office. Security Standard § 2.2.2(d). The clerk's offices must meet certain standards to ensure the security of the records, and they are audited to ensure compliance. Security Standard §§ 2.3.2, 2.3.5. If a clerk's office does not meet the appropriate standard, secure remote access is terminated. Security Standard § 2.3.6.

---

[6] The rules can be found at: http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Rem_Accs_Docs_on_CrtContrd_Websrevision_jam2.pdf (last visited Sept. 8, 2009). This Court may take judicial notice of information on state websites. *Hall v. Virginia*, 385 F.3d 421, 424 n.3 (4th Cir. 2004) (taking judicial notice of website of Virginia Division of Legislative Services).

The cost of remote access varies. For example, the cost for secure remote access to the records for the Circuit Court for the City of Portsmouth is $600 per year. It costs $500 per year for the secure remote access to the Circuit Court records for the City of Alexandria.[7]

There is no statewide plan to redact paper copies of court records. However, the General Assembly has established a "Technology Trust Fund" to assist clerks of court with, among other things, paying for the redaction of SSNs from secure remote access records. *Virginia Code* § 17.1-279(B). The fund consists of an additional $5 fee imposed in each civil action, each instrument to be recorded in the deed books, and each judgment to be docketed in the judgment lien docket book. *Id.* The General Assembly has devoted approximately $7 million to fund the redaction. J.A. 396.

---

[7] Examples of the application forms are available online from the clerks offices in various jurisdictions.
- For the application form for secure remote access for the Circuit Court of the City of Portsmouth, see:
http://www.portsmouthva.gov/CircuitCourtClerk/images/SECURE%20REMOTE%20ACCESS%20SUBSCRIBER%20AGREEME.pdf
- For the application form for secure remote access for the Circuit Court of the City of Alexandria, see:
http://alexandriava.gov/uploadedFiles/clerkofcourt/info/AJISSRASubscriberAgreement.pdf

The General Assembly has set a goal of redacting the SSNs from secure remote access court records by the end of 2010. J.A. 221, 396. The redaction process is being completed either by the clerks of court or by contract work with outside companies. One company, Computing System Innovations, has processed records for 67 Virginia counties. J.A. 280-81. This required the company to process over 49 million images. J.A. 283. The software program that processes these images flags certain images for a manual user to review. J.A. 283, 286-87. The redaction process has a failure rate of between one to five percent. J.A. 397. Documents that are not redacted through this process will be redacted when the clerk is alerted to the presence of the defect. J.A. 397-98.

Although the target date of July 2010 for the redaction of SSNs from records posted on the secure remote access system, the district court found that the process may take longer. J.A. 396-97. Approximately 105 of 120 Virginia jurisdictions have completed the redaction process. J.A. 229, 396. However, some of the State's most populous areas are among the jurisdictions that have not completed the

process. J.A. 396. The 2008 progress report of the Technology Trust Fund details the progress made to date. J.A. 239-258.

## III. THE PLAINTIFF DISPLAYS SOCIAL SECURITY NUMBERS ON HER WEBSITE.

Ostergren advocates for privacy rights in Virginia and nationwide. J.A. 378. She has emphasized the dangers of disseminating public records that contain private information such as SSNs, birth dates, mother's maiden names, financial account numbers and signatures. J.A. 379. Ostergren has lobbied Virginia officials to fund the removal of private information from public records. She also opposes the availability of such information online. J.A. 379.

The plaintiff has posted online public records containing SSNs on her website, www.thevirginiawatchdog.com. J.A. 379. Ostergren explained that she does this to alert members of the public that their own personal information may be online somewhere, as an "object lesson" and for "shock value." J.A. 379.

## IV. OSTERGREN'S WEBSITE IS, IN FACT, USED FOR CRIMINAL ACTIVITY.

As part of his guilty plea in the United States District Court for the District of Connecticut, Case 3:08-cr-00014-VLB, Randy A. Baadhio

stipulated that he submitted fraudulent credit applications to American Express. J.A. 275. He then made unauthorized charges worth at least $142,423.40 on these cards. J.A. 275. Baadhio used fraudulent SSNs to obtain these credit cards. J.A. 275. He obtained some of these names and SSNs from the plaintiff's website, www.thevirginiawatchdog.com. J.A. 275.

After the district court judgment, it has come to counsel's attention that an individual was apprehended in Ghana through a joint investigation of the Ghanaian police and the Department of Homeland Security. This individual confessed to using Ostergren's website to obtain SSNs, and then attempted to blackmail, among other victims, a member of the Virginia House of Delegates. If the Delegate did not pay, the perpetrator threatened to ruin his credit. Counsel has confirmed these facts with the Department of Homeland Security and Ghanaian police via email, and is attempting to obtain official documentation regarding this incident to file with the Court.

## SUMMARY OF ARGUMENT

It is settled law that the First Amendment does not protect all speech in all times and all circumstances. The United States Supreme Court has recognized that a State can curtail speech when the restriction is based on a state interest of the highest order. In this instance, there is no question that by posting SSNs on her website, Ostergren exposes these persons to the very real prospect of the devastating crime of identity theft. This is not an imaginary notion. Criminals have, in fact, been using her website for this very purpose. Protecting citizens or public officials from embarrassment is not a state interest of the highest order. Protecting public officials and citizens from criminal predation is such an interest.

Ordinarily, obtaining information from public records precludes laws that forbid disclosure of that information. Here, the problem with SSNs did not become manifest until after millions of records containing SSNs were filed in public records. It is not possible or desirable to keep the public out of court records, nor is it possible to devise a completely error proof method for eliminating SSNs entirely. Therefore, limiting disclosure is an indispensible component of combating identity theft.

Furthermore, limiting the disclosure of SSNs presents a minimal intrusion that does not affect the essentials of free speech. Ostergren can still vigorously pursue her advocacy. The fact that the law is simple and clear also means that there is no danger of self-censorship of information the public needs to know.

Finally, the district court employed a flawed methodology for determining when a state interest is one of the highest order. Virginia, like other States and the United States government, has taken extensive legislative to limit access to, and dissemination of, SSNs. The State has spent millions of dollars to redact online court records. The risk of grave harm to the victims is clear. The fact that the State could have done more or done things differently to combat the problem does not alter the fact that the interest at issue is one of the highest order.

## STANDARD OF REVIEW

The question before the Court is a legal one, which this Court reviews *de novo*. *In re Morrissey*, 168 F.3d 134, 137 (4th Cir. 1999).

## ARGUMENT

### I. SPEECH THAT CREATES A REALISTIC DANGER OF CRIMINAL PREDATION AND ENABLES OTHER VIOLATIONS OF THE LAW IS NOT PROTECTED BY THE FIRST AMENDMENT.

#### A. The United States Supreme Court's Jurisprudence recognizes that the First Amendment does not protect speech when that speech would transgress a state interest of the highest order.

The First Amendment of the United States Constitution provides in relevant part that "Congress shall make no law . . . abridging the freedom of speech." U.S. Const. amend. 1.[8] The United States Supreme Court has long recognized that "the right of free speech is not absolute at all times and under all circumstances." *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942). *See also Miller v. California*, 413 U.S. 15, 29 (1973) (rejecting "an absolutist, 'anything goes' view of the First Amendment").

Legislative bodies may proscribe certain categories of expression. *Virginia v. Black*, 538 U.S. 343, 359 (2003) (citation omitted). For example, the government can ban advocacy of the use of force or of

---

[8] The First Amendment has been "incorporated" into the Fourteenth Amendment and thereby made applicable to the States. *Stromberg v. California*, 283 U.S. 359, 368 (1931).

violation of the law "where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam). A State can also proscribe "true threats," *Watts v. United States*, 394 U.S. 705, 708 (1969), *i.e.,* "those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals." *Black*, 538 U.S. at 358. States can also ban offers to engage in illegal transactions. *United States v. Williams*, 128 S. Ct. 1830, 1841 (2008). "Fighting words," *i.e.*, those "which by their very utterance inflict injury or tend to incite an immediate breach of the peace" are likewise unprotected. *Chaplinsky*, 315 U.S. at 572. The speech in these categories does not serve the central purposes of the First Amendment, while causing significant societal harms.

With respect to publication of information obtained from the government, the Supreme Court has issued several nuanced and narrow decisions. In *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), the father of a deceased rape victim filed suit for invasion of privacy when a television station made the name of his daughter public.

*Id.* at 474. The television station obtained the name from court records that were open to inspection. *Id.* at 472. Ultimately, the Court held that the First Amendment barred the lawsuit "[u]nder these circumstances." *Id.* at 496-97. The Court made it clear that its ruling was narrow, and that the Court would not

> address the broader question whether truthful publications may ever be subjected to civil or criminal liability consistently with the First and Fourteenth Amendments, or to put it another way, whether the State may ever define and protect an area of privacy free from unwanted publicity in the press.

*Id.* at 491.

The Court reasoned that because the State made the records containing the victim's name public, "the State must be presumed to have concluded that the public interest was thereby being served." *Id.* at 495. The Court further explained that

> [w]e are reluctant to embark on a course that would make public records generally available to the media but forbid their publication if offensive to the sensibilities of the supposed reasonable man. Such a rule would make it very difficult for the media to inform citizens about the public business and yet stay within the law. The rule would invite timidity and self-censorship and very likely lead to the suppression of many items that would otherwise be published and that should be made available to the public. At 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. If there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information. Their political institutions must weigh the interests in privacy with the interests of the public to know and of the press to publish. Once true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it.

*Id.* at 496.

The Court revisited the issue in *Smith v. Daily Mail Publishing Co.,* 443 U.S. 97 (1979). A newspaper had published the name of a juvenile who had been arrested for killing another youth. However, the newspaper did not, as required by West Virginia law, first obtain the written approval of the juvenile court. *Id.* at 100. The Court held that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." *Id.* at 103.

The interest advanced by the State was the protection of the anonymity of a juvenile offender. *Id.* at 104. The Court held that this interest was "not sufficient to justify application of a criminal penalty to respondents." *Id.* at 104. The statute was also faulty because it

targeted newspapers only, allowing radio stations to publish the same information. *Id.* at 104-05. *See also Oklahoma Pub. Co. v. District Court of Oklahoma,* 430 U.S. 308 (1977) (per curiam) (publication of name and photograph of juvenile charged with murder protected by the First Amendment when reporters obtained the information by attending court proceeding); *Bowley v. City of Uniontown Police Dep't*, 404 F.3d 783, 788 (3rd Cir. 2005) (divulging name of juvenile charged with rape was protected by the First Amendment).

In *Florida Star v. B.J.F.,* 491 U.S. 524 (1989), after the Florida Star newspaper published the name of a rape victim, the plaintiff filed a lawsuit against the police department and the Florida Star for violating a statute that prohibited the publication of the name of the victim of a sexual offense. *Id.* at 526. The Court held that the First Amendment protected from liability a newspaper that had published the name of a rape victim when that name was lawfully obtained. *Id.* at 541. However, the Court expressly rejected the "invitation to hold broadly that truthful publication may never be punished consistent with the First Amendment. Our cases have carefully eschewed reaching this ultimate question, *mindful that the future may bring scenarios which*

*prudence counsels our not resolving anticipatorily*." *Id.* at 532 (emphasis added).

Finally, in *Bartnicki v. Vopper*, 532 U.S. 514 (2001), the defendants had obtained from a third party recordings of illegally intercepted communications by the plaintiffs. *Id.* at 519-20. The recordings dealt with ongoing collective-bargaining negotiations between a school board and a teacher's union. The recordings contained embarrassing statements by the plaintiffs. *Id.* at 518-19. The plaintiffs filed suit, relying on a statute that provided financial penalties for persons who intercepted wire communications or who, having reason to know the communication was obtained through an illegal interception, willfully disclosed its contents. *Id.* at 523-24. The newspaper relied on the First Amendment for its defense. *Id.* at 520.

The Court reiterated the applicable test: "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order." *Id.* at 528 (quoting *Daily Mail*, 443 U.S. at 103).

The government asserted two interests in the support of the statute: (1) removing an incentive for parties to intercept private communications, and (2) minimizing the harm to persons hose conversations have been illegally intercepted. *Id.* at 529. The Court rejected the first argument, noting that although "there may be an occasional situation in which an anonymous scanner will risk criminal prosecution by passing on information without any expectation of financial reward or public praise, surely this is the exceptional case." *Id.* at 531. Such unusual scenarios did not constitute a state interest of the highest order. *Id.* at 532.

The Court characterized the second argument as "considerably stronger." *Id.* Ultimately, however, the Court held that "privacy concerns give way when balanced against the interest in publishing matters of public importance." *Id.* at 534. The protracted negotiations over the proper compensation of school teachers were "unquestionably a matter of public concern, and respondents were clearly engaged in debate about that concern." *Id.* at 535. Thus, "as applied to the specific facts of these cases," the application of the statutes "in such circumstances violates the First Amendment." *Id.* at 524-25.

Three key points emerge from these cases. First, the Supreme Court has stressed that its decisions were narrow and fact-bound. Second, the Court has made it clear that the First Amendment does not protect speech when that speech infringes on a state interest of the highest order.[9] Third, the Supreme Court has not addressed a statute similar to this one. There was no indication in *Daily Mail* that the publication of the juvenile defendant's name, the rape victim's name in *Cohn* and *Florida Star*, or the overheated discussions about the looming teacher's strike in *Bartnicki*, exposed any of these individuals to a highly damaging criminal attack.

B. Protecting citizens and public officials from the realistic prospect of a devastating crime, as well as preventing other violations of the law, constitutes a State interest of the highest order.

*Virginia Code* § 59.1-443.2 advances a state interest of the highest order: protecting citizens and public officials from the realistic prospect of devastating criminal predation. In crafting its injunction, the district court acknowledged the obvious and undeniable prospect of identity

---

[9] Notably, in these cases, the Court has eschewed the familiar "strict scrutiny" review of restrictions on First Amendment rights. It is not clear to what degree the strict scrutiny standard differs from the "State interest of the highest order" standard.

theft that is created when SSNs are posted online. The court further acknowledged the devastating consequences that flow from identity theft. J.A. 401-02. This Court has likewise noted that "the harm that can be inflicted form the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous." *Greidinger v. Davis*, 988 F.2d 1344, 1354 (4th Cir. 1993).

There is also no question that SSNs are a key component of stealing someone's identity. By placing these numbers on the internet before a worldwide audience, the plaintiff creates a significant risk of grave harm that does not benefit from constitutional protection.

The danger here is not imaginary. Ostergren's website is, in fact, being used to perpetrate crimes. One criminal has acknowledged in federal court, as part of his guilty plea, that he used Ostergren's website to glean SSNs so he could fraudulently obtain credit cards. J.A. 275. Since the district court rendered its judgment, another example of the criminal use of Ostergren's website has come to light. A defendant in Ghana has acknowledged using Ostergren's website in an effort to blackmail a member of the Virginia House of Delegates.

Other courts have concluded that the First Amendment does not stand in the way of liability when the speech exposes a person to grave harm. *See Capra v. Thoroughbred Racing Association of North America, Inc.*, 787 F.2d 463 (9th Cir. 1986) (lawsuit for invasion of privacy could proceed to the jury when newspaper published the actual name of persons who were in the federal witness protection program); *Hyde v. City of Columbia*, 637 S.W.2d 251 (Mo. Ct. App. 1982) (First Amendment did not bar lawsuit for negligent disclosure of plaintiff's name and address by newspaper, even though newspaper obtained information from the government, when person who abducted her was still at large, and the disclosure constituted a threat to the personal safety of the crime victim).

Finally, although protecting members of the public from identity theft is the chief reason for prohibiting the dissemination of SSNs to the public, there are other important reasons. A private citizen is not the only victim of the crime. Businesses and individuals who are defrauded into providing goods and services must bear the losses associated with identity theft. Moreover, unrestricted posting of SSNs online for the world to see enables criminals to create false identities to escape

detection and apprehension. A false SSN can also allow immigrants to sidestep immigration law. These additional concerns confirm that the state interest at issue here is one of the highest order.

### C. Under the unique circumstances here, the fact that the plaintiff obtained SSNs from government records does not foreclose the State from limiting their dissemination.

As a general proposition, the fact that information was obtained from the government militates against restricting its disclosure. In *Florida Star*, the Court held that "[w]here 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." 491 U.S. at 534 (emphasis added). For example, the Court noted, the government can classify information, or put in place procedures ensuring its redacted release. *Id.* The district court also noted that "the most narrowly tailored solution to the problem of dissemination of SSNs over which the State has custody is not to release those SSNs into the public domain." J.A. 398.

That, however, is simply not an option under the highly unusual circumstances here. When, decades ago, clerks began accepting filings with SSNs, identity theft was simply not an issue. When it did become

a grave problem, millions of documents with SSNs had been filed in court records. It is not possible to redact this many documents overnight and it is not possible to seal off access to court records. Court records have been and must remain open to the public. Real estate records, criminal files and other court records cannot be closed to public access. Furthermore, even when the redaction process of secure remote access is complete, it will not be entirely error proof.[10] Limiting the dissemination of SSNs is, therefore, an indispensible component of solving a very serious problem.

Moreover, there is a significant difference when someone travels to the courthouse in person to view documents, or who signs up for secure remote access by divulging their identity, and someone who places that record on a website for all to see. The person who gains secure remote access or who enters the clerk's office loses the veil of

---

[10] As with the State redaction process, the PACER system employed by the United States court system is not foolproof. For example, searches on the United States Courts PACER electronic filing system "found thousands of documents in which the lawyers and courts had not properly redacted personal information like Social Security numbers, a violation of the courts' own rules." John Schwartz, *An Effort to Upgrade a Court Archive System to Free and Easy*, N.Y. Times, February 12, 2009.

anonymity. Persons using the secure remote access must also pay a fee, and are monitored to ensure they do not engage in improper practices. In contrast, thanks to the plaintiff's website, anonymous viewers anywhere in the world can obtain SSNs and use them for criminal purposes – and, in fact, have done so.

The delicate and fact-specific balancing evident in the Supreme Court's decisions in no way forecloses limits on the dissemination of information even when the information was obtained from the government. For example, suppose that an enterprising investigator uncovers information from government files that would assist a foreign power, or a domestic terrorist, in manufacturing nuclear, biological or chemical weapons of devastating power. It does not follow that the First Amendment would allow publication of such material.[11] *Cf. United States v. Progressive*, 467 F. Supp. 990 (W.D. Wis. 1979) (enjoining the publication of restricted data containing details about the

---

[11] *See, e.g.,* Invention Secrecy Act, 35 U.S.C. §§ 181, 186 (2000) (prohibiting the disclosure of the details of an invention, where the inventions have been ordered to be kept secret because their disclosure would be "detrimental to the national security."); Atomic Energy Act, 42 U.S.C. §§ 2014, 2274 (2000) (prohibiting disclosure of certain data concerning nuclear weapons).

manufacture of nuclear weapons). Likewise, in a situation where a judge, witness, or jury faces a realistic prospect of intimidation or physical harm because of the nature of a case, a court by order or a legislature by statute could proscribe posting information about where the judge, witness, or juror, resides. That is so even if that information is gleaned from the government.

The First Amendment does not require that a State passively accept the fact that its citizens and public officials will be subject to criminal predation. The plaintiff's dissemination of SSNs through her website must yield to the State interest of the highest order.

D. The limited prohibition on disseminating SSNs poses little danger to core expressive speech.

The prohibition imposed by *Virginia Code* § 59.1-443.2 is very straightforward and very limited. It simply forbids the dissemination of SSNs. It thus contrasts with the dangers associated with broad tort concept of invasion of privacy. In *Cohn*, the Court expressed its concern that lawsuits for invasion of privacy would lead to "timidity and self-censorship and very likely lead to the suppression of many items that would otherwise be published and that should be made available to the public." *Cohn*, 420 U.S. at 496. With respect to the statute at issue, the

speaker need not worry about what is prohibited and what is not. All it needs to do is to redact the full SSN from publication.

Prohibiting Ostergren from posting SSNs on her website, and thereby protecting public officials and citizens from victimization, constitutes a *de minimis* restriction on her advocacy. Ostergren can still write extensively about the problems associated with the disclosure of private information in government records, and what is in those records. For example, she could insert stars in place of some of the digits of the SSNs. Such a posting would lose little of its "shock value." By way of analogy, one could criticize the government in World War II for failing to provide adequate escorts to protect convoy ships from submarine attack, without publishing the actual routes of the merchant marine vessels. Because the dangers associated with the actual publication of SSNs are simply too high, the State may prohibit her from posting the actual numbers on her website.

Disseminating SSNs forms "no *essential* part of any exposition of ideas, and [is] of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in" crime prevention. *Chaplinsky*, 315 U.S. at 572

(emphasis added). Where the First Amendment value of the speech is "clearly outweighed" by its societal costs, the speech may be prohibited based on its content. *Chaplinsky*, 315 U.S. at 572. *See also New York v. Ferber*, 458 U.S. 747, 763-64 (1982) (State can prohibit speech where "the evil to be restricted so overwhelmingly outweighs the expressive interests, if any, at stake."). That is the case here.

## II. THE DISTRICT COURT EMPLOYED A FLAWED METHODOLOGY FOR DETERMINING WHEN A GOVERNMENTAL INTEREST IS ONE OF THE HIGHEST ORDER.

Although the district court acknowledged the ravages of identity theft, and indeed permitted the statute to stay in place as to all but a select group of state officials, the court nevertheless concluded that the statute should be enjoined for the plaintiff's website insofar as she posts SSNs of certain state officials. The court reasoned that, in determining whether the interest asserted by the State is one of the highest order, "the State's view and conduct . . . must supply the basis for such a conclusion." J.A. 219. In the district court's view, "the legislative response did not signal that the General Assembly considered protection of SSNs to be an interest of the highest order." J.A. 219. That is because, in the district court's view, the State made certain

records available online before funding redaction of SSNs from these records. J.A. 219. This reasoning is flawed on several levels.

A. Extensive legislative action demonstrates the existence of a State interest of the highest order.

The Virginia General Assembly took extensive action to address the problem of SSNs in public records. As noted above, the General Assembly criminalized identity theft, limited the use and dissemination of SSNs, and allocated millions of dollars to fund redaction from documents available on the secure remote access system.

The United States government and other States also have taken extensive actions to limit the dissemination of SSNs. Many of these state and federal laws, too numerous to mention here, are detailed in a publication of the United States Government Accountability Office. Bovbjerg Statement at 22-29. And, of course, the rules governing United States Courts were amended effective December 1, 2007, to require parties to redact specific categories of information from all filings, including Social Security and taxpayer identification numbers. *See* Fed. R. App. P. 25(a)(5), Fed. R. Civ. P. 5.2, Fed. R. Crim. P. 49.1 and Bankr. R. 9037. This extensive legislative and governmental action demonstrates the great importance of the governmental interest at

stake. *See Ferber*, 458 U.S. at 757-58 (fact that "virtually all of the States and the United States have passed legislation" banning child pornography demonstrated "a government objective of surpassing importance.").

One can always argue that the State should have spent more funds on the problem. But where would those funds come from? Virginia faces daunting budgetary challenges, such as massively underfunded transportation and the rising costs of providing healthcare for Medicaid recipients and state employees, all exacerbated by the current recession. *See, e.g.*, *Virginia's Transportation Mess*, Wash. Post. July 29, 2009 (reporting that "[a] state commission has projected the gap between Virginia's transportation needs and resources over the next 20 years at $100 billion – and that estimate was made five years ago, in much sunnier economic times."). It is easy for a court to view the problem through the focused lens of a particular case, but for the General Assembly, redaction of court records is one of many significant challenges. Virginia has spent millions of dollars to redact SSNs from secure remote access networks and the overwhelming majority of

jurisdictions have completed the redaction process. That hardly signals a lack of concern by the State.

B. The existence of secure remote access does not undermine the nature of the interest at stake.

The district court's criticism of the secure remote access of court records containing SSNs was unwarranted. Virginia provides extensive safeguards to ensure that remote access is for legitimate purposes. Persons wishing to gain access to these records must pay a substantial fee, must apply in person or provide verification of their identity and fill out a detailed application. Each employee must have a separate password. If an employee with access to the records is terminated, the employer must immediately notify the clerk's office. The clerk's offices must maintain the security of the website, and they are audited for compliance. Although the system is not foolproof, it does significantly limit access to these records.

C. Independently of the scope of a State's remedial measures, protection from grave harm is an interest of the highest order.

The district court recognized that limiting exposure to a devastating crime is self-evidently an interest of the highest order. As the court observed,

> the SSN's in the court records are without doubt personal in nature and are entitled to privacy because they are the quintessential personal identifier; and SSNs are susceptible to misuse that can cause great harm, such as identity theft. Therefore, it should not be difficult for a court to conclude that the protection of SSNs from public disclosure should qualify as a State interest of the highest order.

J.A. 219. Even if a State can be criticized for failing to do enough to resolve a problem, the fact that its citizens are exposed to grave harm should suffice to establish a state interest of the highest order.

## CONCLUSION

For the reasons set forth above, the Judgment of the U.S. District Court for the Eastern District of Virginia should be reversed and final judgment entered for the Attorney General.

## ORAL ARGUMENT

The Attorney General respectfully requests oral argument. Oral argument will assist the Court with the complex issues this case presents.

Respectfully submitted,

WILLIAM C. MIMS
Attorney General of Virginia

STEPHEN R. MCCULLOUGH
Virginia State Bar No. 41699
State Solicitor General
smccullough@oag.state.va.us
*Counsel of Record*

WILLIAM E. THRO
Special Counsel

September 8, 2009

MARTIN L. KENT
Chief Deputy Attorney General

STEPHEN M. HALL
Assistant Attorney General

OFFICE OF THE ATTORNEY GENERAL
900 East Main Street
Richmond, Virginia 23219

Telephone: (804) 786-2436
Facsimile: (804) 786-1991

*Counsel for Defendant/Appellant*

**CERTIFICATE OF COMPLIANCE WITH RULE 32(A)**

1. This brief has been prepared using fourteen point, proportionally spaced, serif typeface: Microsoft Word 2007, Century Schoolbook, 14 point.

2. Exclusive of the table of contents, table of authorities and the certificate of service, this brief contains 8029 words.

*/s/Stephen R. McCullough*
Counsel

## CERTIFICATE OF SERVICE

This is to certify that on September 8, 2009, I electronically filed the foregoing OPENING BRIEF with the Clerk of Court using the CM/ECF System, which will send notice of such filing to the following registered CM/ECF users:

Rebecca K. Glenberg, Esquire
Virginia State Bar No. 44099
ACLU of Virginia Foundation, Inc.
530 East Main Street, Suite 310
Richmond, VA 23219
(804) 644-8080
(804) 649-2733 (fax)
rglenberg@acluva.org

*/s/ Stephen R. McCullough*
Counsel