

JAMES BONINI
CLERK

06 MAR -2 PM 5:10

U.S. DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

U.S. DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

DARRELL ESTEP,
14120 Boyd Road
Mount Orab, Ohio 45154

Case No. _____

Judge 1:06 CV 106

Plaintiff,

vs.

J. KENNETH BLACKWELL, in his
official capacity as SECRETARY OF
STATE FOR THE STATE OF OHIO,
180 East Broad Street
Columbus, Ohio 43215

Defendant.

PLAINTIFF'S MOTION FOR TEMPORARY RESTRAINING ORDER
AND
PRELIMINARY INJUNCTION

NOW COMES Plaintiff, Darrell Estep, pursuant to Federal Rule of Civil Procedure 65 and moves the Court for a temporary restraining order and preliminary injunction requiring Defendant to immediately cease and desist from publishing individual social security numbers on the website www.sos.state.oh.us. The grounds for this motion are more fully set forth in the complaint and supporting memorandum filed herewith.

Respectfully submitted,

MARC D. MEZIBOV (Ohio Bar No. 0019316)
CHRISTIAN A. JENKINS (Ohio Bar No. 0070674)
MEZIBOV & JENKINS, CO. LPA
401 East Court Street, Suite 600
Cincinnati, Ohio 45202
Telephone: (513) 723-1600
Telecopier: (513) 723-1620

Trial Attorneys for Plaintiff, Darrell Estep

**MEMORANDUM IN SUPPORT OF MOTION
FOR TEMPORARY RESTRAINING ORDER AND
PRELIMINARY INJUNCTION**

I. Introduction

Plaintiff, Darrell Estep, respectfully requests that the Court issue a temporary restraining order and preliminary injunction requiring Defendant to immediately cease his practice of publishing and making publicly available without any restriction individual social security numbers (“SSNs”) on the website www.sos.state.oh.us which is maintained by Defendant at public expense. As a matter of policy and practice, Defendant publishes via the internet documents containing individual social security numbers and abundant other personal information. The availability of this information without restriction is now well known to criminals as a result of an article published in the Cincinnati Enquirer on March 2, 2006, a copy of which is attached to the complaint as Exhibit D.

There is no legitimate governmental interest in *publishing* individual social security numbers on the internet. It is well established that such publication violates a clearly established right to individual privacy. *See State ex. Rel. Beacon Journal Publishing Company v. City of Akron*, 640 N.E.2d 164 (1994) (“There is a federal right to privacy which protects against governmental disclosure of the private details of one’s life. . . . Due to the federal legislative scheme involving the use of SSNs, city employees have a legitimate expectation of privacy in their SSNs”) *citing Nixon v. Admr. Of Gen. Serv.*, 433 U.S. 425 (1977) and 5 U.S.C. § 552a; *see also Smith v. City of Dayton*, 68 F.Supp.2d 911 (S.D. Ohio 1999) (In releasing this information [names, addresses, phone numbers, social security numbers, drivers licenses, and similar information], the City violated both Officer Smith’s

substantive and procedural due process rights under the Fourteenth Amendment) *citing Kallstrom v. City of Columbus*, 136 F.3d 1055 (6th Cir. 1998). Indeed, Ohio's Attorney General has recognized these same principles in a recent published opinion in which he recommended that public officials redact social security numbers from any documents in their possession before disclosing them. 2005 Ohio Op. Atty. Gen. No. 047, 2005 WL 3598623 (Ohio A.G.)(Attached to Complaint as Ex. E).

Countless individuals stand to become victims of identity theft if the information published by Defendant continues to be made available on the internet without restriction. As a result of such crimes, individual credit is often irreparably damaged and the plaintiff class stands to suffer irreparable harm if the publication continues. (See Clements Affidavit attached as Exhibit A.)¹ Moreover, the public interest in deterring and preventing crime also supports granting the requested relief. There is no legitimate governmental reason to continue indiscriminately publishing social security numbers on the internet. In sum, the requested relief should be granted, and, as there is no risk of harm to anyone from granting the requested relief, no bond should be required.

II. Facts

1. Defendants Have A Policy and Practice of Publishing On the Internet Private Personal Information, Including Social Security Numbers.

The Ohio Secretary of State has maintained a publicly accessible website with the address www.sos.state.ohio.us for several years. The main page of the website contains a

¹ A fully authorized and notarized copy of the affidavit will be separately filed with the Court.

link to search UCC filings which can be searched by individual debtor name, the financing statement or the secured party's name. (Attached hereto as Exhibit B).

Among the documents routinely published on the Defendants' website are UCC filings. Significantly, defendant's website does not include any password protection, such as that utilized by the federal system "PACER," or other safeguard to ensure that only authorized individuals access the personal and confidential information published by Defendants. Thus, plaintiff's private information has been published and made publicly available without any restriction by Defendant.

2. Plaintiff's personal information was published on Defendant's website without his permission.

Mr. Estep financed the purchase of a trailer in 2002, flooring in 2003 and a riding mower in 2004. In each instance the lender prepared and filed a UCC financing statement with Defendant Blackwell's office. The UCC Financing Statements included a section for Mr. Estep's social security number. Redacted copies of the statements are attached to the complaint as Exhibits A, B and C.

Consistent with its policy and practice, Defendant Blackwell's office published the statements filed by Mr. Estep's lenders, including his social security number, on the internet and has allowed unrestricted access to such documents since their filing.

The Secretary of State's Office is responsible for the preservation of hundreds of thousands or millions of documents, and published many of these documents on its website, all in unredacted form without any limitation or restriction on anonymous public access from anywhere in the world.

On March 2, 2006, an article appeared in *The Cincinnati Enquirer* stating that access to individual confidential information, including dates of birth and social security numbers, could be obtained from the Secretary's website. (Attached to Complaint as Exhibit D). According to the article, Secretary Blackwell has been aware of the risk of identity theft created by his office's publication of social security numbers on the internet, but has refused to cease the practice. A spokesperson for Secretary Blackwell's office apparently blames the individuals such as Mr. Estep for the publication of their personal and confidential information, stating that the individuals who filed such forms are "stupid." (see Exhibit D to complaint).

III. Discussion

- 1. A Temporary Restraining Order and Preliminary Injunction Should Be Issued Because It Is Clear That Plaintiff Is Likely To Prevail On The Merits, Because Plaintiff And Many Others Will Suffer Irreparable Harm If The Publication Of Social Security Numbers Continues, And Because The Public Interest Is Served By Preventing Identity Theft.**

Preliminary injunctive relief such as that sought in this case is appropriate under Rule 65 where: 1) there is a likelihood of plaintiff's success on the merits; 2) the plaintiff will suffer irreparable harm without the injunction; 3) others will not suffer harm if the injunction is granted; and, 4) the injunction would serve the public interest. *See In re DeLorean*, 755 F.2d 1223, 1228 (6th Cir. 1985). [T]he four considerations applicable to preliminary injunctions are factors to be balanced and not prerequisites that must be satisfied. These factors simply guide the discretion of the court; they are not meant to be rigid and unbending

requirements. *See In re Eagle-Picher Industries, Inc.*, 963 F.2d 855 (6th Cir. 1992) (citations omitted). Each of these requirements is clearly satisfied on the facts of this case.

1. Likelihood of Success on the Merits

42 U.S.C. § 1983 provides that:

Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress.

To make out a proper claim under § 1983, a plaintiff must show that 1) the action occurred under color of state law, and 2) the action resulted in a deprivation of a constitutional right or a federal statutory right. *See Parratt v. Taylor*, 451 U.S. 527, 535 (1981). The conduct complained of herein was committed by and on behalf of the Ohio Secretary of State who is elected pursuant to O.R.C. § 111.01, and who clearly acted under color of state law by using public funds to create the website and publicly disseminate the personal information of plaintiff and others.

It is well established that citizens of the United States enjoy a fundamental, federal, constitutional right to personal privacy that may not be trammled without a sufficiently compelling public interest. *See Griswold v. Connecticut*, 381 U.S. 479 (1965). This right of privacy necessarily extends to individual social security numbers in today's information driven economy where a social security number coupled with other personal information can afford access to and control over, virtually every facet of one's financial life:

With respect to Social Security numbers, we found a strong privacy interest: the extensive use of Social Security numbers as universal identifiers in both the public and private sectors is one of the most serious manifestations of privacy concerns in the nation. We failed to discover any countervailing public interest justifying their release.

Sheet Metal Workers Int'l Ass'n v. U.S. Dept. of Veterans Affairs, 135 F.3d 891, 898 (3d Cir. 1998), citing *IBEW v. U.S. Dept. of Housing and Urban Dev.*, 852 F.2d 87, 89 (3d Cir. 1988).

The Ohio Supreme Court likewise recognized that the federal constitutional right to privacy extends to social security numbers, which are, of course, created and assigned by an agency of the federal government. See *State ex. Rel. Beacon Journal Publishing Company v. City of Akron*, 640 N.E.2d 164 (1994). Considering a newspaper's challenge to a city's refusal to disclose employee social security numbers under Ohio's Public Records Act (O.R.C. § 149.43), the Ohio Supreme Court found a clear manifestation of this important federal right:

Due to the federal legislative scheme involving the use of SSNs, city employees have a legitimate expectation of privacy in their SSNs. . . . The purpose of the Privacy Act of 1974 was to curtail the expanding use of social security numbers by federal *and local agencies* and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiers. Congress when enacting the Privacy Act of 1974 was codifying the societal perception that SSNs should not be available to all. This legislative scheme is sufficient to create an expectation of privacy in the minds of city employees concerning the use and disclosure of their SSNs.

Id., at 167-68 (emphasis added) citing *Doyle v. Wilson*, 529 F.Supp. 1343, 1348 (Del. 1982).

Ohio's highest court specifically recognized that an intruder using a SSN can quietly discover the intimate details of a victim's personal life without the victim ever knowing of the

intrusion and held that, under the circumstances presented, the Constitution forbade the disclosure of social security numbers as an impermissible invasion of privacy. *Id.*, at 169.

Likewise, the Ohio Attorney General has specifically recognized a constitutional right to privacy in an individual's social security number and advised Ohio's public officials to redact such information from records in their possession before disclosing them. 2005 Ohio Op. Atty. Gen. No. 047, 2005 WL 3598623 (Ohio A.G.). Other courts are in accord. *See e.g. Arakawa v. Sakata*, 133 F.Supp.2d 1223, 1229 (D. Hawaii 2001) ("The public release of a SSN could lead to problems related to credit card fraud or identity theft...access to an individual's medical, financial, or other sensitive records; records that have become all the easier to obtain thanks to the Internet." The court also found that it could not "conceive of any state interest...sufficient to outweigh Plaintiff's privacy rights in his SSN."); *Kirkland v. Sheehan*, 2001 WL 1751590 at *6-7 (Wash. Super. 2001) ("Access to an individual's SSN enables a new holder to obtain access to and to control, manipulate or alter other personal information. In effect, access to an SSN allows a person, agency or company to more efficiently and effectively search for and seize information and assets of another, a power originally available only to the government and one which was subject to direct Constitutional restraint Keeping Social Security numbers private is a compelling interest for the government and citizens alike [T]he disclosure of a public employee's Social Security number would be . . . not of legitimate concern to the public.") (internal citations and quotations omitted); *Meyerson v. Prime Realty Services, LLC*, 796 N.Y.S.2d 848, 854 (N.Y. Sup. Ct. 2005) (examining the history of social security numbers and finding that social security numbers are not only confidential information but that social security numbers are protected by "a privilege against disclosure.")

The posting of documents containing social security numbers is part of Defendant's official policy and practice. Thus, Defendant may be properly held responsible for the harm caused by the invasion of plaintiff's privacy. See *Monell v. New York City Dept. of Social Services*, 436 U.S. 658, 690 (1978). The essential elements of plaintiff's claim are clearly present because his federal constitutional right to privacy was violated under color of state law pursuant to Defendant's official policy. Accordingly, plaintiff has demonstrated a substantial likelihood of success on the merits.

2. Irreparable Harm

Social Security numbers are a special kind of personal information.² For identity thieves, "[t]he most highly sought information is personal data, such as *Social Security numbers*, bank account or credit card numbers, telephone calling card numbers and other valuable identifying data." RONALD N. WEIKERS ET AL., DATA SECURITY AND PRIVACY LAW: COMBATING CYBERTHREATS § 1:7 (Robert D. Brownstone, et al., supplemented 2005) (emphasis added)(attached).

² The courts have long recognized the special importance of a Social Security number. See e.g. *Greidinger v. Davis*, 988 F.2d 1344, 1353-54 (4th Cir. 1993):

"For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck. Elizabeth Neuffer, *Victims Urge Crackdown on Identity Theft*, BOSTON GLOBE, July 9, 1991, at 13, 20 (In Massachusetts, "[a]uthorities say that, with another person's Social Security number, a thief can obtain that person's welfare benefits, Social Security benefits, credit cards or even the victim's paycheck."); Michael Quint, *Bank Robbers' Latest Weapon: Social Security Numbers*, N.Y. Times, September 27, 1992, at 7 (SSN can be used to order new checks at a new address). In California, reported cases of fraud involving the use of SSNs have increased from 390 cases in 1988 to over 800 in 1991. Y. Anwar, *Thieves Hit Social Security Numbers*, San Francisco *1354 Chronicle, August 30, 1991, A1, A2. Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous. These are just examples, and our review is by no means exhaustive; we highlight a few to elucidate the egregiousness of the harm."

Much of the harm occasioned by Defendant's website probably goes undetected for months or even years. *Beacon Journal Publishing v. Akron*, 640 N.E.2d 164 (Ohio 1994). Victims of identity theft are sometimes left to settle the hefty bills run up by their alter egos or fight lengthy legal battles with creditors. Moreover, the impact upon a victim's credit status can be permanent and is virtually irremediable. Thus, plaintiff and members of the putative class stand to be irreparably harmed if the publication of his social security numbers is not stopped. (Clements Affidavit).

3. Public Interest

The public interest is obviously served by preventing identity theft. An injunction stopping Defendant's publication of social security numbers will also serve the public's interest by limiting the damages that Defendant is responsible to pay to plaintiff and the class he represents.

2. No Bond Should Be Required Because The Requested Relief Does Not Pose A Threat Of Harm To Defendant Or Anyone Else.

The court may decline to require any bond when issuing a temporary restraining order or preliminary injunction. This is especially true where there is no realistic likelihood of harm to Defendant from enjoining his or her conduct. *See Jorgensen v. Cassidy*, 320 F.3d 906 (9th Cir. 2003). No appreciable purpose is served by publishing individuals' social security numbers on the internet. Indeed, nothing in the Ohio Revised Code requires Defendant to operate such a website. Accordingly, no harm will be done to anyone by directing Defendant to cease publication of social security numbers. If Defendant believes that there is a significant public purpose, he can redact social security numbers from all such

documents before posting them to the internet in the future. However, for the present time, no harm will befall anyone except those who use Defendant's website as part of a criminal endeavor. Accordingly, no bond should be required.

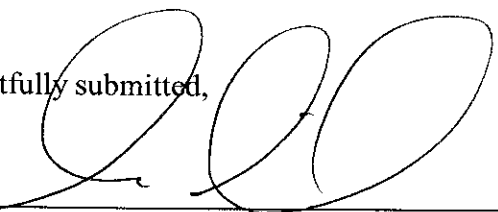
3. The Court May And Should Grant Injunctive Relief With Respect To The Entire Proposed Class.

Although no class has yet been certified pursuant to Rule 23, under the circumstances the Court is empowered to treat this case as a class action for purposes of fashioning injunctive relief and consider the irreparable harm faced by putative class members. *See Helwig v. Kelsey-Hayes Co.*, 857 F.Supp. 1168, 1180 (E.D.Mich. 1994), *citing Lapeer County Medical Care Facility v. Michigan*, 765 F.Supp. 1291, 1301 (W.D.Mich. 1991) (prior to certification, court treated case as class action); *Musto v. American General Corp.*, 615 F.Supp. 1483, 1492 (W.D. Tenn. 1985) (preliminary injunction may issue prior to certification), *rev'd on other grounds*, 861 F.2d 897 (6th Cir. 1988), *cert. denied*, 490 U.S. 1020 (1989). Because injunctive relief is so clearly appropriate and in the public interest under the circumstances, the Court should exercise this authority and fashion preliminary injunctive relief in favor of the entire proposed class.

IV. Conclusion

Unfortunately, a large amount of personal information has already been provided to potential criminals by the Defendant. Thus, the Court should grant plaintiff the requested temporary restraining order and preliminary injunction and direct Defendant to immediately cease the publication of documents containing individuals' social security numbers.

Respectfully submitted,



MARC D. MEZIBOV (Ohio Bar No. 0019316)
CHRISTIAN A. JENKINS (Ohio Bar No. 0070674)
MEZIBOV & JENKINS, CO. LPA
401 East Court Street, Suite 600
Cincinnati, Ohio 45202
Telephone: (513) 723-1600
Telecopier: (513) 723-1620

Trial Attorneys for Plaintiff, Darrell Estep