

SUPREME COURT OF NEW JERSEY  
DOCKET NO. 63,258

FRED BURNETT, :  
Plaintiff-Petitioner, : Civil Action  
 :  
v. : On Appeal from  
 : Superior Court,  
COUNTY OF BERGEN and : Appellate Division  
BERGEN COUNTY CLERK'S : No. A-2002-06T2  
OFFICE, :  
Defendants-Respondents :  
 :

---

BRIEF of *AMICI CURIAE*  
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY  
and PRIVACY RIGHTS CLEARINGHOUSE

---

GRAYSON BARBER, ESQ.  
GRAYSON BARBER, LLC  
68 Locust Lane  
Princeton, NJ 08540  
(609) 921-0391

EDWARD BAROCAS  
AMERICAN CIVIL LIBERTIES UNION  
OF NEW JERSEY FOUNDATION  
P.O. Box 32159  
Newark, NJ 07102  
(973) 642-2086

Attorneys for *Amici Curiae*  
ACLU-NJ and Privacy Rights Clearinghouse

TABLE OF CONTENTS

	<u>Page</u>
STATEMENT OF INTEREST OF AMICI CURIAE . . . . .	1
ARGUMENT . . . . .	2
I. THE APPELLATE DIVISION CORRECTLY HELD THAT SOCIAL SECURITY NUMBERS ARE DUE PRIVACY PROTECTIONS AND SHOULD NOT BE DISCLOSED. . . . .	3
A. Pursuant to OPRA and New Jersey Supreme Court Precedent, Information in Which Citizens Have a Reasonable Expectation of Privacy Should not be Disclosed by the Government Without An Overriding Interest for So Doing. . . . .	4
B. Social Security Numbers Are Due an Extremely High Degree of Protection, As Evidenced By State and Federal Statutes that Prohibit or Limit Their Disclosure . . . . .	7
C. The Commercial Use of SSNs by Data Aggregators and Others Have Created Worldwide Privacy Concerns Including Identity Theft. . . . .	12
D. There Is No Overriding Justification to Disclose SSNs. . . . .	17
CONCLUSION . . . . .	20

TABLE OF AUTHORITIES

<u>Case Cited</u>	<u>Page</u>
<u>Asbury Park Press v. Ocean County Prosecutor's Office</u> , 864 A.2d 446 (Law Div. 2004) . . . . .	19
<u>Casey v. Male</u> , 63 N.J. Super. 255 (Co. Ct. 1960) . . . . .	3
<u>Doe v. Portiz</u> , 142 N.J. 1 (1995) . . . . .	3, 4, 6, 7
<u>Elvis Presley Enterprises, Inc. v. Capece</u> , 950 F. Supp. 783 (S.D. Tex. 1996) . . . . .	17
<u>Heights Comm. Congress v. Virginia</u> , 732 F.2d 526 (6 <sup>th</sup> Cir. 1984) . . . . .	10
<u>Int'l Bd. Of Elec. Workers Local 5 v. Dep't of Housing &amp; Urban Dev.</u> , 852 F.2d 87 (3d Cir. 1998) . . . . .	9
<u>Judicial Watch, Inc., v. Dep't of Justice</u> , 365 F.3d 1108 (D.C. Cir. 2004) . . . . .	9
<u>Mason v. City of Hoboken</u> , 951 A.2d 1017 (2008) . . . . .	18
<u>NLRB v. Illinois Am. Water Co.</u> , 933 F.2d 1368 (7 <sup>th</sup> Cir. 1991) . . . . .	10
<u>Olmstead v. United States</u> , 277 U.S. 438 (1927) . . . . .	6
<u>Painting Ind. of Hawaii Market Recovery Fund v. U.S. Dep't of Air Force</u> , 26 F.3d 1479 (9 <sup>th</sup> Cir. 1994) . . . . .	9
<u>Sheet Metal Workers Int'l Assn. v. U.S. Air Force</u> , 63 F.3d 994 (10 <sup>th</sup> Cir. 1995) . . . . .	9
<u>Sherman v. Dep't of Army</u> , 244 F.3d 357 (5 <sup>th</sup> Cir. 2001) . . . . .	9
<u>South Jersey Pub. Co. v. N.J. Expressway Auth.</u> , 124 N.J. 478 (1991) . . . . .	19
<u>State v. Hemepele</u> , 120 N.J. 182 (1990) . . . . .	6
<u>State v. McAllister</u> , 184 N.J. 1 (2005) . . . . .	6

<u>Sterling v. Borough of Minersville</u> , 232 F.3d 190 (3 <sup>rd</sup> Cir. 2000) . . . . .	6
<u>Taxpayers Assoc. of Weymouth Twp. v. Weymouth Twp.</u> , 80 N.J. 6 (1976), cert. denied, 430 U.S. 977 (1977). . . . .	3
<u>U.S. v. Westinghouse</u> , 638 F.2d 570 (1980) . . . . .	6, 7
<u>Whalen v. Roe</u> , 429 U.S. 589, 605 (1977) . . . . .	3
<u>Yeager v. Hackensack Water Co.</u> , 615 F. Supp. 1087 (D.N.J. 1985) . . . . .	10

<u>Federal Statutes and Codes Cited</u>	<u>Page</u>
5 U.S.C. 552 . . . . .	8
5 U.S.C. 552a . . . . .	9, 15
15 U.S.C. 1681 . . . . .	15
18 U.S.C. 2710 . . . . .	15
42 U.S.C. 405 . . . . .	7, 8

<u>State Statutes and Codes Cited</u>	<u>Page</u>
410 ILCS 535/11 . . . . .	12
Ariz. Rev. Stat. § 25-121 . . . . .	12
Burns Ind. Code Ann. § 16-37-3-9 . . . . .	12
Burns Ind. Code Ann. § 31-11-4-4 . . . . .	12
Cal. Fam. Code § 2024.5 . . . . .	12
Cal Health & Saf Code § 102231 . . . . .	12
Cal Health & Saf Code § 102425 . . . . .	12
Idaho Code § 67-3007 . . . . .	12

K.S.A. § 65-2409a . . . . .	12
Ky. Rev. Stat. Ann. 402.100 . . . . .	12
La. R.S. 9:224 . . . . .	12
La R.S. § 23:1671 . . . . .	12
MCL § 333.2813 . . . . .	12
Minn. Stat. § 144.215 . . . . .	12
Miss. Code Ann. § 41-57-14 . . . . .	12
Mo. Rev. Stat. § 193.075 . . . . .	12
Mo. Rev. Stat. § 454.440 . . . . .	12
Mont. Code Ann. § 40-1-107 . . . . .	12
N.D. Cent. Code § 23-02.1-28 . . . . .	12
N.J.A.C. 13:45F-4.1 . . . . .	10-11
N.J.S.A. 17:23A-1 . . . . .	15
N.J.S.A. 47:1A-1 et seq. . . . .	4, 5, 17
N.J.S.A. 56:8-162 et seq. . . . .	10
Ohio Rev. Code Ann. § 3101.05 . . . . .	12

## STATEMENT OF INTEREST OF AMICI CURIAE

The American Civil Liberties Union of New Jersey ("ACLU-NJ") is a private non-profit, non-partisan membership organization dedicated to the principle of individual liberty embodied in the Constitution. Founded in 1960, the ACLU-NJ has nearly 15,000 members in the State of New Jersey. It strongly supports ensuring the transparency of government as well as ensuring individuals' rights to informational privacy. It has participated in numerous legal cases seeking to further both principles. The ACLU-NJ is the state affiliate of the American Civil Liberties Union, which was founded in 1920 for identical purposes, and is composed of nearly 500,000 members nationwide.

The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organization with a two-part mission -- consumer information and consumer advocacy. Based in San Diego, California, it is primarily grant-supported and serves individuals nationwide. One of PRC's primary goals is to raise awareness of how technology affects personal privacy. It provides numerous practical tips on how to protect personal privacy on its web site, [www.privacyrights.org](http://www.privacyrights.org).

The participation of *amici curiae* will assist this Court in the resolution of the issues of public importance raised by this case by providing the legal context, both state and federal, in which to analyze the facts of this case. The participation of

amici is particularly appropriate in cases with "broad implication," Taxpayers Assoc. of Weymouth Twp. v. Weymouth Twp., 80 N.J. 6, 17 (1976), *cert. denied*, 430 U.S. 977 (1977), or in cases of "general public interest." Casey v. Male, 63 N.J. Super. 255, 259 (Co. Ct. 1960). This is such a case.

#### ARGUMENT

*Amici* offer this brief to inform the Court of existing legal authorities that limit the use and disclosure of Social Security numbers (SSNs).

The SSN has a distinctive status which carries with it inherent privacy risks. Social Security numbers are unique to each individual, have become mandatory for many basic transactions in the United States, and can therefore serve as a pathway to one's identity and activities. Indeed, no other form of personal identification plays such a significant role in linking records that contain sensitive information. Government agencies (and data aggregators) should bear a measure of accountability for their treatment of SSNs.

To discern the metes and bounds of such accountability, this Court should look to widely accepted principles that form the basis of most privacy laws in New Jersey, the United States and elsewhere. Indeed, as explained in Section I.B. below, numerous state and federal statutes place limitations on

governmental disclosure of SSNs that may create liability applicable to Bergen County in this instance.

**I. THE APPELLATE DIVISION CORRECTLY HELD THAT SOCIAL SECURITY NUMBERS ARE DUE PRIVACY PROTECTIONS AND SHOULD NOT BE DISCLOSED.**

Generally, the public should have access to government records, and *amici* fully support making public information more accessible. Indeed, confidence in government at all levels is best sustained by access to the information necessary to promote the vigorous public discussion that a well-functioning democracy requires.

However, our state requires its citizens to disclose a great deal of information about their personal affairs; such information can include our Social Security numbers, medical information and financial information. The government may well have important interests in obtaining such information. However, as noted by the United States Supreme Court, "the right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures." Whalen v. Roe, 429 U.S. 589, 605 (1977). Therefore a state, after collecting such information, must "evidence a proper concern with, and protection of, the individual's interest in privacy." Id. See also Doe v. Portiz, 142 N.J. 1, 78 (1995) (the right to confidentiality "encompasses



two strands: 'the right to be free from the government disclosing private facts about its citizens and from the government inquiring into matters in which it does not have a legitimate and proper concern.'" ). This concomitant duty to protect privacy was directly incorporated into the terms of OPRA itself. N.J.S.A. 47:1A-1.

When dealing with information that individuals reasonably expect to remain private, such as SSNs, the presumption is that such information is to remain confidential unless there is an overriding justification for its disclosure. Id.; see also Doe v. Poritz, 142 N.J. at 78. As it relates to government records requests under OPRA, such an overriding justification for disclosure doesn't normally exist unless the disclosure of the sensitive personal information is itself necessary to shed light on the functioning of government.

**A. Pursuant to OPRA and New Jersey Supreme Court Precedent, Information in Which Citizens Have a Reasonable Expectation of Privacy Should not be Disclosed by the Government Without An Overriding Interest for So Doing.**

In enacting OPRA, the Legislature recognized that, while the goal of the statute was to promote the public's right of access to government information,

a public agency has a responsibility and an obligation to safeguard from public access a citizen's personal information with which it has been entrusted when disclosure thereof would violate the citizen's reasonable expectation of privacy.

N.J.S.A. 47:1A-1.

This requirement mirrors the constitutional privacy requirement cited above that, when the government obtains sensitive information from its citizens, it carries a concomitant responsibility not to unnecessarily or improperly disclose protected information.

Indeed, the right to privacy confers, "as against the government, the right to be let alone--the most comprehensive of rights and the right most valued by civilized men." State v. Hemele, 120 N.J. 182, 225, 576 A.2d 793 (1990), quoting Olmstead v. United States, 277 U.S. 438, 478 (1927) (Brandeis, J., dissenting); see also Doe v. Poritz, 142 N.J. at 100; Sterling v. Borough of Minersville, 232 F.3d 190 (3<sup>rd</sup> Cir. 2000) (quoting same). It encompasses an "individual interest in avoiding disclosure of personal matters," Whalen v. Roe, 429 U.S. at 599, and a measure of control over "knowledge about oneself." U.S. v. Westinghouse, 638 F.2d 570, 577, n.5 (1980). The New Jersey Constitution provides even greater privacy protections than does the federal constitution. See, e.g., State v. McAllister, 184 N.J. 1 (2005); State v. Hemele, supra.

Where, as here, there is a reasonable expectation of privacy in the information being disclosed, the Court "must decide whether the intrusion on the right of privacy is

justified, balancing the governmental interest in disclosure against the private interest in confidentiality." Doe, 142 N.J. at 78. More specifically, this Court has applied the balancing test set forth in Westinghouse, 638 F.2d at 577 n.5, to determine whether an individual's interest in privacy outweighs the public interest in disclosure. Doe v. Poritz, 142 N.J. at 88. The Westinghouse test includes analyzing the nature of the information being disclosed, the potential for harm arising from nonconsensual disclosure, and statutory mandates or articulated public policy regarding disclosure.<sup>1</sup>

As set forth below, the nature of the information at issue is extremely sensitive, the nonconsensual disclosure of SSNs creates a serious risk of harm to citizens, and there is no strong public interest in disclosure that would override the right to privacy.

---

<sup>1</sup> The full list of factors to consider are:

the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access. [Westinghouse, 639 F.2d at 578.]

As such, the disclosure of the SSNs at issue in this case would violate New Jersey citizens' constitutional right to privacy. Further, it could subject Bergen County to liability for violating federal or state statutes, as explained below.

**B. Social Security Numbers Are Due an Extremely High Degree of Protection, As Evidenced By State and Federal Statutes that Prohibit or Limit Their Disclosure.**

Recognizing the sensitivity of SSNs, Congress and the New Jersey Legislature have empowered, or tried to empower, state actors like Bergen County to protect the privacy of SSNs it obtains. The standards embodied in the federal and state statutes should inform this Court's analysis as to the expectation of privacy and to the nature of the individual privacy interest at stake.

**1. The Social Security Act**

The Social Security Act bars disclosure by federal, state and local governments of SSNs collected pursuant to laws enacted on or after October 1, 1990. 42 U.S.C. 405(c)(2)(C)(viii). In the Act, Congress recognized the vulnerability of the SSN and amended the Social Security Act to restrict disclosures, by local governments as well as by the federal government. Recent amendments provide criminal penalties for "unauthorized willful

disclosures" of SSNs; the Department of Justice would determine whether to prosecute a willful disclosure violation.<sup>2</sup>

## 2. The Freedom of Information Act

Ironically, one of the federal statutes most protective of SSNs is the Freedom of Information Act, 5 U.S.C. 552. "Exemption Six" contains an exception for "information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. 552(b).

Under this exemption, courts have consistently held that SSNs are to be withheld from public requestors, and therefore will not be released, or will be redacted. See, e.g., Sherman v. Dep't of Army, 244 F.3d 357 (5<sup>th</sup> Cir. 2001) (incidental appearance of SSNs); Judicial Watch, Inc., v. Dep't of Justice, 365 F.3d 1108 (D.C. Cir. 2004); Sheet Metal Workers Int'l Assn. v. U.S. Air Force, 63 F.3d 994 (10<sup>th</sup> Cir. 1995) (denying union access to employees' SSNs); Painting Ind. of Hawaii Market Recovery Fund v. U.S. Dep't of Air Force, 26 F.3d 1479 (9<sup>th</sup> Cir. 1994) (same); Int'l Bd. Of Elec. Workers Local 5 v. Dep't of

---

<sup>2</sup> The Social Security Act specifically cites willful disclosures, hence careless behavior or inadequate safeguards may not be subject to criminal prosecution. The relevant provision also applies only to disclosure of SSNs collected in accordance with laws enacted on or after October 1, 1990. For SSNs collected by government entities pursuant to laws enacted more than 18 years ago, this provision does not apply and therefore, would not restrict disclosing the SSN. It is also unclear whether the provision applies to disclosure of SSNs collected without a statutory requirement to do so.

Housing & Urban Dev., 852 F.2d 87, 89 (3d Cir. 1998) (same);  
Heights Comm. Congress v. Virginia, 732 F.2d 526 (6<sup>th</sup> Cir. 1984)  
(names and SSNs of federal loan recipients redacted). But see  
NLRB v. Illinois Am. Water Co., 933 F.2d 1368 (7<sup>th</sup> Cir. 1991).

### **3. The Privacy Act of 1974**

The Privacy Act of 1974 was designed to discourage improper uses of SSNs. Yeager v. Hackensack Water Co., 615 F. Supp. 1087, 1091 (D.N.J. 1985). The report of the Senate Committee supporting adoption of the Act states the use of SSNs as universal identifiers in both the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." S. Rep. No. 93-1183, as reprinted in 1974 U.S.C.C.A.N. 6196, 6943.

One section of the federal Privacy Act of 1974 applies to state and local governments. Section 7 makes it unlawful for federal, state, and local agencies to deny an individual a right or benefit provided by law because of the individual's refusal to disclose his SSN. Pub. L. No. 93-579, §7, 88 Stat. 1896, 1909 (1974), reprinted in 5 U.S.C. § 552a note (2003).

### **4. The Identity Theft Protection Act**

The New Jersey Legislature similarly restricted disclosures of SSNs in the Identity Theft Prevention Act ("ITPA"), P.L. 2005, c. 226. Recognizing the dangers of widespread use of SSNs, the New Jersey Legislature imposed restrictions in the ITPA,

providing that "no person, including any public or private entity, shall: ... intentionally communicate or otherwise make available to the general public an individual's Social Security number." N.J.S.A. 56:8-164. The ITPA specifically provides that every business or public entity must destroy SSN records by making them "unreadable, undecipherable, or nonreconstructable." NJSA 56:8-162. Bergen County cannot realistically shred land title documents, but it must at least redact SSNs.

Not only does the ITPA prohibit government and commercial actors from displaying SSNs, (see N.J.S.A. 56:8-164), it requires businesses to notify customers whose SSNs are disclosed as a result of security breaches. N.J.S.A. 56:8-163. Also, pursuant to this statute, when disclosures are sought, the disclosing entities must at least give citizens fair warning. Using DataTrace as an example, the company must alert consumers to DataTrace's practices of procuring and re-selling SSNs.

The Division of Consumer Affairs adopted rules on April 7, 2008, to implement the ITPA. N.J.A.C. 13:45F-4.1 et seq. With respect to SSNs, the rules provide strict limitations that would prohibit the type of disclosure DataTrace seeks from Bergen County. Id.<sup>3</sup>

---

<sup>3</sup> With respect to SSNs, the rules provide:

(a) No person, including a public or private entity, shall:

## 5. State efforts to limit use of SSNs in government records

Numerous states have recognized that commercial data brokers obtain SSNs from many sources, including public records that individuals are required to file in order to enjoy important rights and privileges offered by society. States around the country have therefore sought to limit access to SSNs

---

1. Publicly post or publicly display an individual's Social Security number or any four or more consecutive numbers taken from the individual's Social Security number;
2. Print an individual's Social Security number on any materials that are mailed to the individual, unless State or Federal law requires the Social Security number to be on the document to be mailed;
3. Print an individual's Social Security number on any card required for the individual to access products or services provided by the person or public or private entity;
4. Require an individual to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; or
5. Require an individual to use his or her Social Security number to access an Internet website, unless a password or unique PIN or other authentication device is also required to access the Internet web site.

While the rule contains an exception for information required to be disclosed under OPRA, as noted herein, SSNs should not to be disclosed under OPRA based on the "reasonable expectation of privacy" citizens hold in SSNs.



in those records. For instance, marriage licenses have been a source for SSNs, and a number of states have enacted legislative protections to prevent their disclosure. See, e.g., Ariz. Rev. Stat. § 25-121; Cal. Fam. Code § 2024.5; Burns Ind. Code Ann. § 31-11-4-4; Ky. Rev. Stat. Ann. 402.100; La. R.S. 9:224; 19-A M.R.S. § 651; MCL § 333.2813; Mont. Code Ann. § 40-1-107; Ohio Rev. Code Ann. § 3101.05. Likewise, several states limit the appearance of SSNs on birth records. See Cal Health & Saf Code § 102425; 410 ILCS 535/11; K.S.A. § 65-2409a; 22 M.R.S. § 2761; Minn. Stat. § 144.215; Miss. Code Ann. § 41-57-14; Mo. Rev. Stat. § 193.075; Mo. Rev. Stat. § 454.440. Others restrict SSN disclosure in records associated with death. See Cal Health & Saf Code § 102231; Idaho Code § 67-3007; Burns Ind. Code Ann. § 16-37-3-9; La R.S. § 23:1671; N.D. Cent. Code § 23-02.1-28.

**C. The Commercial Use of SSNs by Data Aggregators and Others Have Created Worldwide Privacy Concerns Including Identity Theft.**

By allowing SSNs to become public, the government subjects them to commercial and other uses. Indeed, once made public, the information cannot be retrieved; and once disseminated, there is no way to put the cat back in the bag.<sup>4</sup>

---

<sup>4</sup> *Amici* disagree with the Appellate Division's inference that the reason for the request or the identity of the requestor should be taken into account in analyzing whether information should be disclosed. Burnett v. County of Bergen, 402 N.J. Super. 319, 340 (App. Div. 2008). First, under OPRA itself, it is improper for the government to inquire into the identity of a requestor or the reasons behind a request, and then make a

Once released publicly, SSNs will be subjected to sale over the Internet by information brokers. "As long as criminals can buy a list of names and SSNs through an Internet auction, we will continue to be plagued by the consequences." Testimony of the Inspector General of the Social Security Administration before the Subcommittee on Social Security of the House Committee on Ways and Means, July 10, 2003, <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=655>

There is an increasing body of evidence that identity thieves visit government Web sites to find SSNs in order to use them to obtain employment, credit cards and wireless phone accounts. "Social Security Numbers: More Could Be Done to Protect SSNs," GAO-06-586T, March 2006, available at [www.gao.gov](http://www.gao.gov).

Five years ago, a Federal Trade Commission report found that nearly 10 million Americans, or nearly 5 percent of US adults, had been victimized by identity theft in 2002. [www.ftc.gov/os/2003/09/synovaterreport.pdf](http://www.ftc.gov/os/2003/09/synovaterreport.pdf); see also "Counterfeit identification and identification fraud raise security concerns: Hearing before the Senate Committee on Finance, 108<sup>th</sup> Cong.

---

judgment as to whether the reason is sufficient. See, e.g., N.J.S.A. 47:1A-5(b) ("A copy or copies of a government record may be purchased by *any person*") (emphasis added); N.J.S.A. 47:1A-5(f) (permitting anonymous requests). Second, information should either be public or not, and a requestor's identity is of no import to that determination.

(Sept. 9, 2003) (Statement of Robert J. Cramer, Managing Director, Office of Special Investigations, US General Accounting Office).

The effects on victims range from financial losses to lost jobs, and even in some cases to the arrest of innocent people who are "wanted" for crimes committed by others using their identities. In most cases, victims must spend hours trying to get commercial data aggregators to correct their records and stop propagating false information.

The consequences of unfettered data mining fall on everyone, not just victims of identity theft. Data brokers use SSNs from various sources to create consumer profiles that contribute to irresponsible lending, "one of the overlooked causes of the debt boom and the resulting crisis, which threatens to choke the global economy." Brad Stone, "Banks Mine Data and Woo Troubled Borrowers," New York Times, October 22, 2008.

The cure is to be found in legal principles that are already codified in law. There presently exist standards that have become the foundation for statutes in the United States, Canada and Europe. These standards, known as the "principles of fair information practices," are not about "privacy" so much as the perceived tug-of-war (or creative tension) between freedom of information and individual privacy. See Personal Privacy in

an Information Society: The Report of the Privacy Protection Study Commission, U.S. Gov't Printing Office, July 1977.

Numerous federal and state statutes embrace the principles of fair information practices, but cover narrow segments of personal information. See, e.g., Fair Credit Reporting Act, 15 U.S.C. 1681 (1970) (credit); Video Privacy Protection Act, 18 U.S.C. 2710 (1988) (video rentals); Privacy Act, 5 U.S.C. 552a (1974) (federal government records); New Jersey Information Practices Act, N.J.S.A. § 17:23A-1 (1985) (insurance records).

Europe and Canada treat freedom-of-information and privacy together. Every state in the European Union has adopted the principles of fair information practices as law. See Council Directive 95/46/EC, 1995 O.J. (L 281), 31-51 (EC) (Directive of the European Parliament and the Council of Ministers of the European Commission on the protection of individuals with regard to the processing of personal data and on the free movement of such data); The Organisation for Economic Cooperation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2005), available at [http://www.oecd.org/document/18/0,2340,en\\_2649\\_201185\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html). Canada's statute is called the "Personal Information Protection and Electronic Documents Act," R.S.C., ch. P 21, §§ 10, 12 (1985).

Moreover, citizens should have a remedy if their SSNs are misused. Arguably, citizens have a proprietary interest in their own SSNs. If Elvis Presley's heirs can prevent someone from using his name on a bar or restaurant to make money, Elvis Presley Enterprises, Inc. v. Capece, 950 F. Supp. 783, 801-02 (S.D. Tex. 1996), an ordinary citizen should be able to prevent the commercial use of his name through the sale of his name and SSN. See Flavio L. Komuves, "We've Got Your Number: an Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers," 16 J. Marshall J. Computer & Info. L. 529, 574 (1998).<sup>5</sup>

Legislative and judicial efforts seek to protect SSNs despite commercial data aggregators attempts to explore many avenues to obtain them. See Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information, GAO-04-11 (January 2004). This Court should not allow OPRA requests to circumvent these efforts.

---

<sup>5</sup> At a minimum, data aggregators should bear a responsibility to treat sensitive personal information with care. It cannot avail to claim that the data came from government records and therefore a) must be accurate, and b) can be used for any and all purposes. Recent security breaches show that databases containing legally collected SSNs are often inadequately protected against accidental or intentional disclosure. [www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)

**D. There Is No Overriding Justification to Disclose SSNs.**

Citizens should feel confident that when the government requires us to provide it with sensitive personal information such as our SSNs, it will disclose that information only to authorized employees and those who need to see the numbers for the performance of their duties.<sup>6</sup>

OPRA does not support a finding of a public interest in, much less an overriding need for, public disclosure of SSNs. Indeed, the public policy underlying OPRA is to shed light on the operation of government agencies in New Jersey, not to publish information about individuals. See N.J.S.A. 47:1A-1. As held by this Court: "OPRA's purpose is to maximize public knowledge about public affairs in order to ensure an informed citizenry and to minimize the evils inherent in a secluded process.'" Mason v. City of Hoboken, 951 A.2d 1017, 1025 (N.J.

---

<sup>6</sup> Beyond the question of disclosure, government entities should also provide citizens with reasons for collecting our SSNs and how they intended to use our SSNs. Preferably, governments should collect our SSNs directly from us. When collecting SSNs is allowed, but not required, it should be done only as reasonably necessary for the proper administration of lawful activities. Further, government entities should develop policies and security plans for protecting SSNs. If there is an overriding need (which is here non-existent) to share SSNs with others, it should prohibit those third parties from re-disclosing SSNs except as required by law. These duties should apply not only to government entities, but to commercial entities when SSNs are required for business transactions.

2008) (quoting Asbury Park Press v. Ocean County Prosecutor's Office, 864 A.2d 446 (N.J. Super. Ct. Law Div. 2004)).<sup>7</sup>

Disclosure of SSNs does not further that purpose. The effect of disclosing SSNs that the government obtained for inclusion in land title documents would be solely to disclose personal information about individuals, as such information sheds no light on the conduct of a public agency or official or on other governmental matters of significance to the public.<sup>8</sup>

*Amici* recognize that there are times when arguably sensitive information about individuals can be disclosed (specifically, when it would in fact shed light on government functions). For example, while it is not appropriate to disclose financial information regarding a private individual simply because it might have been required on a particular

---

<sup>7</sup>This is consistent with New Jersey's general public policy pertaining to disclosure of government information which, as this Court has explained, involves "access to sufficient information to enable the public to understand the reasonableness of the public body's action." South Jersey Pub. Co. v. N.J. Expressway Auth., 124 N.J. 478, 494-95 (1991) (addressing request for information under the Open Public Meetings Act and OPRA's predecessor (the Right to Know Law)).

<sup>8</sup> Land title records have been in the public domain from time immemorial, for many reasons. A distinction may be drawn, however, between the public information in land title records and personal information that is recorded for extraneous (or purely administrative) purposes. Unless they serve the purposes for which land title records are placed in the public domain, SSNs are extraneous or, at the very least, is information that can be obtained by the government but not disclosed.

government form, it is appropriate to disclose the salaries of public employees. However, it is hard to fathom when disclosure of SSNs would shed light on the function of government (or, in the constitutional context, when the public need for disclosure outweighs the inherent privacy interest at stake). Regardless of whether such a hypothetical situation may exist, the present context is clearly not such a case.

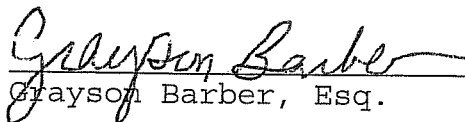
As the need for disclosure does not outweigh the individual interest in privacy and the risk of harm inherent in public disclosure of SSNs, the Appellate Division's decision should be affirmed.



**CONCLUSION**

The federal government, numerous state governments including New Jersey, and the courts have sought to ensure the public's right to privacy in their SSNs. This Court should not allow OPRA requests to circumvent those efforts. The public information in land title records must be available through OPRA requests, without exposing SSNs.

For the reasons set forth herein, the Appellate Division's decision should be affirmed

  
\_\_\_\_\_  
Grayson Barber, Esq.

  
\_\_\_\_\_  
Edward Barocas, Esq.

Attorneys for Amici Curiae

Dated: November 10, 2008