

NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE APPELLATE DIVISION

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-2002-06T2

FRED BURNETT,

Plaintiff-Appellant,

v.

COUNTY OF BERGEN and
BERGEN COUNTY CLERK'S OFFICE,

Defendants-Respondents.

APPROVED FOR PUBLICATION

August 22, 2008

APPELLATE DIVISION

Argued October 24, 2007 – Decided August 22, 2008

Before Judges Wefing, Parker and Coleman.

On appeal from the Superior Court of New Jersey, Law Division, Bergen County, Docket No. L-6482-06.

Richard Gutman argued the cause for appellant.

John M. Carbone argued the cause for respondents (Carbone and Faasse, attorneys; Mr. Carbone, on the brief).

Michael J. Fasano argued the cause for amicus curiae New Jersey Land Title Association (Lomurro, Davison, Eastman & Munoz, attorneys; Mr. Fasano, on the brief).

The opinion of the court was delivered by

PARKER, J.A.D.

Plaintiff Fred Burnett appeals from an order entered on December 4, 2006 directing defendants Bergen County and the

Bergen County Clerk's Office to submit a written bid detailing the costs of copying the government records requested by plaintiff under the Open Public Records Act (OPRA). Plaintiff appeals from those paragraphs of the order requiring defendants to redact and remove social security numbers (SSNs) from the records; requiring each document be watermarked¹ with the copying date; and denying plaintiff's request for counsel fees and costs. We affirm.

Plaintiff is an employee of Data Trace Information Systems (DTIS), "a national title technology company that creates computer-based searching tools for the title insurance industry." DTIS operates "land record databases for over 200 counties in 25 states." According to Kathleen Donovan, the Bergen County Clerk, DTIS "is a compiler and reseller of public and private information which is compiled and gathered on individuals." Plaintiff represents the interests of his employer, DTIS.

In September 2003, plaintiff filed a complaint with the Government Records Council (GRC), an administrative body created under OPRA as an alternative to the Superior Court for

¹ Watermarking is the process of inserting onto a microfilmed record a non-removable date of copying and a disclaimer that the record is not official.

addressing access to public records. N.J.S.A. 47:1A-6 and -7. On April 4, 2006, plaintiff withdrew his GRC complaint after two years of litigation because he believed he would not prevail before the GRC and wished "to minimize further uncertainty and delay."

On April 17, 2006, plaintiff filed a Government Records Request Form with the Bergen County Clerk, requesting "microfilm copies of the rolls of microfilm containing the follow[ing] recorded and filed documents from the Books listed below, from the corresponding Beginning Book Number through the most current book." The request named thirteen kinds of realty documents, including deeds, liens, and various mortgage-related documents. Plaintiff grounded his request in OPRA and the common law.

Christine Healey, who is responsible for the information and technology services in the Bergen County Clerk's Office, stated in her certification that plaintiff's request seeks "approximately [eight million] pages of documents which are stored on an estimated 2,559 rolls of archival microfilm." Healey certified that the job would cost in excess of \$460,000. Because the Clerk's Office does not have record-imaging technology to allow identification and redaction of SSNs, each microfilm document must be copied to paper or an electronic format.

On April 25, 2006, Donovan advised plaintiff of two deficiencies in his request: (1) it was not filed with the "centralized custodian of the designated records" as required by OPRA; and (2) his ending date for production of the documents was not sufficiently specific. Nevertheless, the Clerk accepted the request and explained the procedure for obtaining bids from an outside vendor to do the copying. She asked plaintiff to choose one of the two procedures for processing the request.

On May 5, 2006, plaintiff responded, choosing a bid process and clarifying the order of copying that he preferred. On May 10, Donovan confirmed the bidding procedure and stated that the copies "will all contain the disclaimer and watermarking as we have discussed."

On May 22, 2006, plaintiff complained that Donovan had not yet advised him of the date on which he could expect to receive the bid. He also denied any agreement with respect to disclaimers and watermarkings, explaining that any discussions had been during settlement negotiations in the prior OPRA proceedings before the GRC and that no agreement had been reached.

In August 2006, plaintiff filed a verified complaint and order to show cause seeking to compel defendants to provide microfilmed copies of all land title records from 1984 to the

present. The records sought in the complaint were the same as those specified in plaintiff's April 17, 2006 OPRA request.

On October 25, 2006, the order to show cause was argued in the trial court. After hearing the arguments, Judge Sybil R. Moses rendered a decision on the record ordering defendants to provide the requested records with all SSNs redacted at plaintiff's expense. The trial court found that while the records were accessible under both OPRA and the common law, the right of access did not extend to SSNs appearing on the documents.

Judge Moses noted that "[a] citizen's right . . . to access the public records is not absolute." In determining whether the information sought under OPRA must be released, Judge Moses identified three issues to be considered. First, whether the requested material constituted a public record; second, whether the request sufficiently described the documents sought; and third, the gravamen of plaintiff's claims, whether the law exempted disclosure of SSNs, requiring their redaction before releasing the nearly eight million pages of documents. Judge Moses found that the parties did not dispute that the requested records were public records under OPRA and that plaintiff's request was adequate. Judge Moses began her analysis of the third issue by stating:

When analyzing an OPRA request, and whether or not Social Security numbers are exempt from disclosure I will interpret OPRA in [pari materia] with New Jersey, federal, and sister state statutes and regulations to determine if the requested information is considered confidential, and whether access to the information is inimical to the public interest.

Quoting Michelson v. Gannett, 379 N.J. Super. 611, 621 (App. Div. 2005), the judge commented that "[w]hen the requested material appears on its face to encompass legislatively recognized confidentiality concerns, a court should presume that the release of the government record is not in the public interest." The judge considered Asbury Park Press v. Ocean County Prosecutor's Office, 374 N.J. Super. 312, 331 (Law Div. 2004), in determining that the Legislature intended to prevent disclosure of information -- specifically SSNs -- in "those instances in which a person had a reasonable expectation of privacy."

The judge also considered the Identity Theft Prevention Act (ITPA), passage of which was pending at the time of argument, and the laws of Connecticut and New York addressing identity theft. The judge noted that "[o]ther states, including the Federal Government, have already enacted[,] or are in the process of [enacting,] similar privacy laws to increase the

protection of Social Security numbers." Judge Moses concluded that

considering the most recent legislative action, considering the law in sister states, protect[ing] Social Security numbers, considering all of the legislation, which is either pending or has been enacted . . . the public interest is implicated in this. . . . [A]ccordingly, I conclude that it is against the public interest to enable theft identity to be encouraged and take place.

The judge also addressed plaintiff's request under a common law analysis. In applying the balancing test articulated by the New Jersey Supreme Court in Loigman v. Kimmelman, 102 N.J. 98 (1986), Judge Moses determined "the effect that disclosure of Social Security numbers may have on citizens of this county . . . who put their Social Security numbers on deeds, liens, [and] mortgages . . . is significant." She concluded that plaintiff's commercial interest in social security numbers was outweighed by the government's interest in maintaining the confidentiality of its citizens' Social Security numbers (SSNs).

An order memorializing Judge Moses' decision was entered on December 4, 2006. Plaintiff filed a timely notice of appeal. The New Jersey Land Title Association was granted amicus curiae status and submitted a brief in support of plaintiff's position. In this appeal, plaintiff argues that the trial court erred in (1) ordering redaction of SSNs; (2) ordering the insertion of a

watermark on each document; and (3) denying its application for counsel fees.

I

The Legislature and the courts have consistently struggled to maintain a balance between the public's right to know and the individual's right to privacy with respect to certain personal information. Here, the question posed is whether a private, commercial enterprise has the right to gather SSNs in order to compile a database for sale to other private, commercial entities for profit.

A. The New Jersey Statutes

In 2002, the Legislature enacted the Open Public Records Act (OPRA), N.J.S.A. 47:1A-1 to -13, replacing New Jersey's Right to Know Law, N.J.S.A. 47:1A-2 to -4, which was "built on the State's longstanding public policy favoring ready access to most public records."² Serrano v. South Brunswick Twp., 358 N.J. Super. 352, 363 (App. Div. 2003). New Jersey's public policy favors "access to sufficient information to enable the public to understand and evaluate the reasonableness of the

² In replacing the Right to Know Law with OPRA by L. 2001, c. 17, the Legislature retained much of the original statement of legislative purpose and findings in N.J.S.A. 47:1A-1. See Hartz Mountain Indus., Inc. v. New Jersey Sports & Exposition Auth., 369 N.J. Super. 175, 183, n.2 (App. Div.), certif. denied, 182 N.J. 147 (2004).

public body's action." South Jersey Pub. Co. v. N.J. Expressway Auth., 124 N.J. 478, 494-95 (1991); accord, Kuehne Chem. Co., Inc. v. N. Jersey Dist. Water Supply Comm'n, 300 N.J. Super. 433, 438 (App. Div.), certif. denied, 151 N.J. 466 (1997).

In OPRA, the Legislature declared that "government records shall be readily accessible for inspection, copying, or examination by the citizens of this State, with certain exceptions, for the protection of the public interest."

N.J.S.A. 47:1A-1. The Legislature also declared that

[A]ll government records shall be subject to public access unless exempt from such access by [N.J.S.A. 47:1A-1 et seq.] . . . any other statute; resolution of either or both houses of the Legislature; regulation promulgated under the authority of any statute or Executive Order[;] . . . Rules of Court; any federal law, federal regulation or federal order.

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

The courts should narrowly construe exceptions to the right of access. Serrano, supra, 358 N.J. Super. at 363.

The Legislature, however, tempered public access rights with its finding and declaration that "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. Moreover,

"[b]alancing public access rights and privacy rights in a reasonable and reasoned manner has been an important part of our Judiciary's tradition." Associate Justice Barry T. Albin, Report of the Supreme Court Special Committee on Public Access to Court Records, 25 (2007).

Under OPRA, the term "government record" does not include that portion of any document which discloses a person's SSN. N.J.S.A. 47:1A-1.1. Prior to allowing access to a government record, the government custodian of that record must redact that portion of the document disclosing the SSN unless the SSN is part of a record "required by law to be made, maintained or kept on file by a public agency." N.J.S.A. 47:1A-5a.

There is no dispute that the realty records sought by plaintiff are government records statutorily required to be maintained on file by the county recording officer and that SSNs are part of those records, thereby falling within the OPRA exception to non-disclosure of SSNs. See N.J.S.A. 46:19-1; Dugan v. Camden County Clerk's Office, 376 N.J. Super. 271 (App. Div.); certif. denied, 184 N.J. 209 (2005). Plaintiff argues, therefore, that OPRA itself requires the SSNs to be released. In our view, however, there are competing interests that must be balanced before we can determine whether SSNs included in the

records should remain unredacted in documents plaintiff seeks to gather, compile and sell to other users.

In 2005, the Legislature obviously recognized the danger of disclosing SSNs in public documents and adopted N.J.S.A. 47:1-16, effective October 1, 2005. The statute provides that "No person, including any public or private entity, shall print or display in any manner an individual's Social Security number on any document intended for public recording with any county recording authority." N.J.S.A. 47:1-16(a). Prior to recording a document, the recording authority must "delete, strike, obliterate or otherwise expunge" a SSN on a document that has been presented for recording. N.J.S.A. 47:1-16(b). These provisions do not apply, however, to documents originating with a court or taxing authority; documents that when filed by law constitute a non-consensual lien against an individual; any publicly recorded documents required by law to contain a SSN; or any documents filed with or recorded by a County Surrogate. N.J.S.A. 47:1-16(c). In other words, the realty documents filed with the county clerks and sought by plaintiff are excepted from the required redaction of SSNs under N.J.S.A. 47:1-16(a).

The Legislature went even further to protect SSNs in adopting the ITPA, effective January 1, 2006. In enacting the ITPA, the Legislature declared that

g. Social Security numbers are frequently used as identification numbers in many computer files, giving access to information an individual may want kept private and allowing an easy way of linking data bases. Therefore, it is wise to limit access to an individual's Social Security number whenever possible; and

h. It is therefore a valid public purpose for the New Jersey Legislature to ensure that the Social Security numbers of the citizens of the State of New Jersey are less accessible in order to detect and prevent identity theft and to enact certain other protections and remedies related thereto and thereby further the public safety.

[N.J.S.A. 56:11-45(2).]

The ITPA further provides that:

No person, including any public or private entity, shall:

(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; [or]

. . . .

(4) Intentionally communicate or otherwise make available to the general public an individual's Social Security number.

[N.J.S.A. 56:8-164a.]

This provision, however, does not apply to documents required to be maintained under OPRA. N.J.S.A. 56:8-164e.

In 2004, the State created the Privacy Study Commission (Commission) as a result of OPRA to study (1) "the disclosure of

home addresses and telephone numbers;" (2) the "commercial use of public information held by public agencies;" and (3) "the impact of technology on privacy concerns." N.J. Privacy Study Commission Final Report (December 2004) at 1 (Privacy Study). Interestingly, the Commission did not discuss concerns about disclosure of SSNs in filed documents because it apparently believed that they were already protected under OPRA. Id. at 25, n.27.

In Higg-A-Rella, Inc. v. County of Essex, 141 N.J. 35, 44 (1995), the New Jersey Supreme Court curtailed disclosure of personal information in tax records -- specifically exempt from redaction under N.J.S.A. 47:1-16(b) -- when it held that because counties and municipalities were not required to maintain computerized tax lists, the computer tapes of the tax records requested by the plaintiff were not considered records "required to be made or maintained" and, therefore, not "Right-to-Know public documents." The Court noted that "'[t]he consolidated magnetic tape or tapes are merely "a convenient means" by which the county board can perform its mandated functions.'" Ibid. (quoting Higg-A-Rella, Inc. v. County of Essex, 276 N.J. Super. 183, 187-88 (App. Div. 1994)). The fact that plaintiff sought the government records for a commercial purpose was not considered in the court's analysis. Here, plaintiff seeks

"microfilm copies of the rolls of microfilm" maintained by the county clerk. As in Higg-A-Rella, microfilm is merely "a convenient means" of storing recorded documents.

B. Federal Statutes

In considering whether an individual has an expectation of privacy in his or her SSN under federal law, we look to the Social Security Act, the FOIA, and the Privacy Act of 1974.

Originating in 1935, a SSN is a nine-digit account number assigned by the Commissioner of Social Security to assist in carrying out the Social Security laws. See 42 U.S.C.A. § 405(c)(2)(B). SSNs were originally intended for the federal government's exclusive use as a method of tracking earnings to determine the amount of Social Security taxes to credit each worker's account. Greidinger v. Davis, 988 F.2d 1344, 1352 (4th Cir. 1993).

SSNs received federal statutory protection from disclosure after amendments were made to the Social Security Act in 1990. This protection, however, applies to those SSNs that are "obtained or maintained by authorized persons pursuant to any provision of law enacted on or after October 1, 1990." 42 U.S.C.A. § 405(c)(2)(C)(viii)(I). "Social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on

or after October 1, 1990, shall be confidential, and no authorized person shall disclose any such social security account number or related record." Ibid.

SSNs collected by government entities pursuant to laws enacted before October 1, 1990 have also found protection from disclosure as an unwarranted invasion of privacy. See, e.g., I.B.E.W. Local Union No. 5 v. United States Dep't of Hous. & Urban Dev., 852 F.2d 87, 88-89 (3d Cir. 1988), mod. on other grounds sub nom. Sheet Metal Workers Int'l Ass'n v. United States Dep't of Veterans Affairs, 135 F.3d 891 (3rd Cir. 1998).

In 1966, Congress enacted the Freedom of Information Act (FOIA), 5 U.S.C.A. § 552. Broadly conceived, the FOIA "seeks to permit access to official information long shielded unnecessarily from public view and attempts to create a judicially enforceable public right to secure such information from possibly unwilling official hands." EPA v. Mink, 410 U.S. 73, 80, 93 S. Ct. 827, 832, 35 L. Ed. 2d 119, 128 (1973).

In considering whether SSNs fall under Exemption 6 of the FOIA, the Third Circuit Court of Appeals explained that

[E]mployees have a strong privacy interest in their Social Security numbers. Congress has recognized this privacy interest by making unlawful any denial of a right, benefit, or privilege by a government agency because of an individual's refusal to disclose his Social Security number." Privacy Act of 1974, Pub. L. 93-579, § 7, 88

Stat. 1896, 1909 (1974), reprinted in 5 U.S.C. § 552a note (1982). Moreover, in its report supporting the adoption of this provision, the Senate Committee stated that 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." S. Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6943.

[I.B.E.W. Local Union No. 5, supra, 852 F.2d at 89 (emphasis added).]

The court had no hesitation concluding that the release of employees' SSNs contained in government payroll records "constitute[d] a clearly unwarranted invasion of privacy and [was] therefore barred by Exemption 6" given that there was "no countervailing public interest." 852 F.2d at 89.

The federal Privacy Act of 1974 (Privacy Act) provides "certain safeguards for an individual against an invasion of personal privacy." Privacy Act of 1974, Pub. L. No. 93-579, § 2, 88 Stat. 1896 (1974), reprinted in 5 U.S.C.A. § 552a, note.³ In adopting the Privacy Act, Congress found that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States." Ibid. Moreover, "the

³ The Privacy Act contains several provisions that were not codified but may be found under the Historical and Statutory Notes to 5 U.S.C.A. § 552a. See Pub. L. No. 93-579, § 7(1)(a), 88 Stat. 1896 (1974); McKay v. Thompson, 226 F.3d 752, 755 (6th Cir. 2000), cert. denied, 532 U.S. 906, 121 S. Ct. 1230, 149 L. Ed. 2d 139 (2001).

increasing use of computers and sophisticated information technology . . . has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information." Ibid.

With that purpose in mind, Section 7 of the Privacy Act attempts to limit the use by federal, state and local agencies of an individual's SSN by making it unlawful for any of these agencies to deny an individual a right, privilege or benefit because of the refusal to disclose a SSN. 5 U.S.C.A. § 552a, note. The legislative history surrounding Section 7 suggests Congress sought to curtail both federal and local government agencies from expanding use of SSNs. The congressional purpose underlying Section 7 was to eliminate the threat to individual privacy and confidentiality posed by the compelled disclosure of one's SSN. S. Rep. No. 1183, 93d Cong., 2d Sess., reprinted in 1974 U.S. Code Cong. & Admin. News 6916, 6943.

C. Constitutional Protections

We next look to the constitutional protections for individual privacy. The New Jersey Supreme Court has recognized that "[w]ith its declaration of the right to life, liberty and the pursuit of happiness, Article I, § 1 of the New Jersey Constitution encompasses the right of privacy." Doe v. Poritz, 142 N.J. 1, 89 (1995). The right of privacy has been defined as

"the right of an individual to be . . . protected from any wrongful intrusion into his private life which would outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities." McGovern v. Van Riper, 137 N.J. Eq. 24, 32 (Ch. 1945), aff'd 137 N.J. Eq. 548 (E & A 1946). "[H]aving its origin in natural law, . . . [i]t is one of the 'natural and inalienable rights' recognized in article 1, section 1 of the constitution of this state." Id. at 33.

There have been a number of circumstances in which our Supreme Court has found a constitutional right of privacy, including the disclosure of confidential or personal information. See Hennessey v. Coastal Eagle Point Oil Co., 129 N.J. 81, 96 (1992) (citing In re Martin, 90 N.J. 295, 318, 324-25, (1982) (balancing disclosure of personal information against government's need for information)). Recently, for example, the New Jersey Supreme Court recognized that "citizens have a reasonable expectation of privacy . . . in the subscriber information they provide to Internet service providers." State v. Reid, 194 N.J. 386, 389 (2008).

In Martin, the Court adopted a balancing test to settle conflicting interests between the government's need for personal information and an individual's right of confidentiality. 90 N.J. at 318; accord Doe, supra, 142 N.J. at 90. "'The

legitimate public interest must be considered . . . in balance with the competing right of privacy on the part of the affected individuals.'" Martin, supra, 90 N.J. at 318 (quoting Lehrhaupt v. Flynn, 140 N.J. Super. 250, 260 (App Div. 1976), aff'd o.b., 75 N.J. 459 (1978)). The Court concluded that "'even if the governmental purpose is legitimate and substantial . . . the invasion of the fundamental right of privacy must be minimized by utilizing the narrowest means which can be designed to achieve the public purpose.'" Ibid. (quoting Lehrhaupt, supra, 140 N.J. Super. at 262).

Relying on United States Dep't of Defense v. Federal Labor Relations Auth., 510 U.S. 487, 114 S. Ct. 1006, 127 L. Ed. 2d 325 (1994), Exemption 6 of the Freedom of Information Act (FOIA), and Aronson v. Internal Revenue Serv., 767 F.Supp. 378 (D. Mass. 1991), mod. by 973 F.2d 962 (1st Cir. 1992), the Doe Court confirmed that the public disclosure of an individual's home address implicates privacy interests. 142 N.J. at 82.

The Court found that merely because an individual's home address may be publicly available does not inevitably lead to the conclusion that no privacy interest is implicated:

It is true that home addresses often are publicly available through sources such as telephone directories and voter registration lists, but "[in] an organized society, there are few facts that are not at one time or another divulged to another." The privacy

interest protected by Exemption 6 "encompass[es] the individual's control of information concerning his or her person." An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.

[Id. at 83 (emphasis added) (quoting Federal Labor Relations, supra, 510 U.S. at 501, 114 S. Ct. at 1015, 127 L. Ed. 2d at 337) (citations omitted).]

The Court framed the issue -- not as whether the individual had a privacy interest in his address -- but as whether the inclusion of his address, along with other personal information, implicated any privacy interest. Id. at 83 (citing Aronson, supra, 767 F.Supp. at 389, n.14) (noting that disclosure of a home address "can invite unsolicited contact or intrusion based on the additional revealed information.").

In State v. McAllister, 184 N.J. 17 (2005), the New Jersey Supreme Court held that, under the New Jersey Constitution, a citizen has a reasonable expectation of privacy in his or her bank records, 184 N.J. at 29, even though "the Federal Constitution does not recognize an expectation of privacy in bank records and does not give citizens recourse to challenge the federal government's acquisition of their bank records from their banks, even if that acquisition involves egregious misconduct." 184 N.J. at 26 (citing United States v. Miller,

425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976); United States v. Payner, 447 U.S. 727, 100 S. Ct. 2439, 65 L. Ed. 2d 468 (1980)).

In reaching its decision, the Court recognized that "difficulties can arise when state law deviates from federal law" but it acknowledged that "our state courts may create 'an independent body of state constitutional law.'" McAllister, supra, 184 N.J. at 29 (quoting State v. Hunt, 91 N.J. 338, 362-63 (1982) (Handler, J., concurring)). "[W]hen the United States Constitution affords our citizens less protection than does the New Jersey Constitution, we have not merely the authority to give full effect to the State protection, we have the duty to do so.'" Ibid. (quoting State v. Hemepele, 120 N.J. 182, 196 (1990)).

Bank records, on their face, "are simply a collection of numbers, symbols, dates and tables." McAllister, supra, 184 N.J. at 30. The Court expressed concern, however, that "when compiled and indexed, individually trivial transactions take on a far greater significance." Ibid. "In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography.'" Id. at 30-31 (quoting Burrows v. Superior Court, 13 Cal.3d 238

(1975)). "'A bank customer may not care that employees of the bank know a lot about his financial affairs, but it does not follow that he is indifferent to having those affairs broadcast to the world or disclosed to the government.'" Id. at 31 (quoting Richard Posner, The Economics of Justice 342 (1981)). The Court emphasized the "need to protect ordinary citizens' financial privacy in ways that promote fairness." Id. at 32.

In our view, citizens' concerns about disclosure of their social security numbers to a commercial entity for the purpose of compiling a database for sale to other commercial entities for profit is as great -- if not greater -- than the concerns a bank customer may have at "having his financial affairs broadcast to the world or disclosed to the government." Ibid.

D. The Other State and the Federal Courts

In addition to our own law, we look to other state and federal courts that have addressed disclosure of personal information, including SSNs. In Whalen v. Roe, 429 U.S. 589, 605, 97 S. Ct. 869, 879, 51 L. Ed. 2d 64, 77 (1977), the United States Supreme Court stated:

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of

the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. 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.

[Emphasis added.]

The Fourth Circuit Court of Appeals in Greidinger, supra, 988 F.2d at 1354, held that a Virginia law requiring voter registrants to disclose their SSNs on the applications and making those records subject to public disclosure imposed an "intolerable burden" upon the right to vote. The court recognized that since the enactment of the federal Privacy Act in 1974, "an individual's concern over his social security number's confidentiality and misuse has become significantly more compelling." Id. at 1353. In identifying the potential harm that could result from the disclosure of a SSN, the court warned that

[A]rmed with one's social security number, 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. . . . Succinctly stated, the harm that can be inflicted from the disclosure of a social security number to an unscrupulous individual is alarming and potentially financially ruinous.

[Id. at 1353-54.]

The Ohio Supreme Court found that "disclosure of the social security numbers would violate the federal constitutional right to privacy." State ex rel. Beacon Journal Publ'g Co. v. City of Akron, 640 N.E.2d 164, 165-166, reconsideration denied by 642 N.E.2d 388 (Ohio 1994). There, pursuant to Ohio's open public records statute, the plaintiff, an Ohio newspaper, requested computer tape records of Akron's master employee files that contained employees' names, addresses, SSNs, birthdates and other employment information. Ibid. The tape was provided with the SSNs redacted. Ibid. When the plaintiff objected, the Ohio Supreme noted "the Privacy Act of 1974 codified the societal perception that SSNs should not . . . be . . . available to all. The 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 168

Heavily influenced by the potential misuse of SSNs, the Ohio Court commented:

While the release of all city employees' social security numbers would provide inquirers with little useful information about the organization of their government, the release of the numbers could allow an inquirer to discover the intimate, personal details of each city employee's life, which are completely irrelevant to the operations of government. As the Greidinger court warned, a person's SSN is a device which can

quickly be used by the unscrupulous to acquire a tremendous amount of information about a person.

[Id. at 169.]

Ultimately, the Ohio Court concluded that the United States Constitution prohibited disclosure of city employees' SSNs under the circumstances of that case. Ibid.

The courts of Kansas, Kentucky and Pennsylvania, the federal district of Massachusetts and Eastern District of New York have also found the disclosure of SSNs to be a violation of an individual's privacy. See, e.g., Data Tree, LLC v. Meek, 109 P.3d 1226, 1237-38 (Kan. 2005); Zink v. Commonwealth, 902 S.W.2d 825, 829 (Ky. Ct. App. 1994) (holding that the privacy interests substantially outweigh the "negligible" public interest in disclosure); Tribune-Review v. Allegheny County Hous., 662 A.2d 677, 683 (Pa. Commw. Ct. 1995) (holding that public access to government records containing an individual's SSN "may not be at the expense of the individual's right to privacy"); Aronson v. Internal Revenue Serv., 767 F. Supp. 378, 388 (D. Mass. 1991) (denying the release of Social Security numbers even though they would undoubtedly make it easier for a commercial service to find those to whom tax refunds are due); Oliva v. U.S. Dep't of Hous. and Urban Dev., 756 F.Supp. 105, 107 (E.D.N.Y. 1991) (finding that release of SSNs and dates of birth for individuals

on HUD's Mutual Mortgage Insurance/Mortgage Insurance Premium list constitutes a "clearly unwarranted invasion of personal privacy" under Exemption 6 of the FOIA).

These cases recognize the significance of SSNs and the potential for serious damage to an individual whose SSN is misused. Data Tree, supra, 109 P.3d at 1238 (noting that SSNs are "often used as identifiers for financial accounts or for obtaining access to electronic commerce"); Zink, supra, 902 S.W.2d at 829 (stating that "[a]ccess to a wealth of data compiled by both government agencies and private enterprises such as credit bureaus is obtainable simply upon presentation of the proper social security number."); Tribune-Review, supra, 662 A.2d at 683 (noting that "when a social security number is misused it can destroy a life.").

In Data Tree, a case very similar to one before us, a data-mining company brought a declaratory judgment action and sought injunctive relief against a Kansas county register of deeds, alleging that the county register was violating the Kansas Open Records Act (KORA) by redacting personal information and demanding fees for the redaction of information such as SSNs, mothers' maiden names, and dates of birth, from bulk records requested under KORA. 109 P.3d at 1226. Under KORA, a public agency need not disclose public records containing "information

of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy."

Id. at 1233. In balancing the competing interests, the Kansas Supreme Court stated

An individual's social security number, date of birth, and mother's maiden name are often used as identifiers for financial accounts or for obtaining access to electronic commerce. Most people would consider this information of a "personal nature." The United States Supreme Court, interpreting the FOIA, stated that information is "private if it is intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public." . . . We see no reasons why social security numbers, mothers' maiden names, and dates of births do not fall into this privacy realm.

[Id. at 1238 (quoting Reporters Committee, supra, 489 U.S. at 763-64, 109 S. Ct. at 1476-77, 103 L. Ed. 2d at 789-90.) (citations omitted).]

The Kansas Supreme Court acknowledged Data Tree's argument -- similar to plaintiff's argument here -- that an individual would have a lesser expectation of privacy in documents filed with the Kansas Register of Deeds because it acts as the depository of documents specifically for public notice. Ibid. The information being sought by Data Tree, however, was not for public notice but for commercial purposes -- similar to plaintiff's purposes here -- and the Court found that "[t]he public interest to be served by releasing unredacted documents

with social security numbers, mothers' maiden names, and dates of births to a data collection company [intending] to sell this information for a profit is at best insignificant." Ibid. The Kansas Court concluded: "where disclosure of the personal or private information fails to significantly serve the principal purpose of the [state's open records act], nondisclosure is favored." Ibid.

A Kentucky appellate court employed a similar analysis in Zink, when it determined that an individual's privacy interests in his or her personal information, such as a SSN appearing on a public record "substantially outweigh[ed] the negligible . . . public interest . . . in disclosure." 902 S.W.2d at 829-30. Recognizing that a SSN "today represent[s] no less than the keys to an information kingdom as it relates to any given individual," the court reasoned that the purpose of disclosure, focusing on the citizens' right to be informed about government activities, was not fostered by the "disclosure of information about private citizens that is accumulated in various government files that reveals little or nothing about an agency's own conduct." Id. at 829.

E. Balancing of Interests

When diverse pieces of information, such as a name, SSN, address, bank or mortgage holder and simulated signature, are assembled into a package -- as they are in the records sought by plaintiff to be compiled in a database and sold for commercial purposes -- a privacy interest is implicated. See Doe, supra, 142 N.J. at 87. Under these circumstances, the SSN becomes a key to access a myriad of information about an individual, such as government filings containing a person's physical description, race, nationality, gender, family life, marital relationship, residence, location, contact information, political activity, financial condition, employment, criminal history, health and medical condition, and other personal information. Daniel J. Solove, MODERN STUDIES IN PRIVACY LAW: NOTICE, AUTONOMY AND ENFORCEMENT OF DATA PRIVACY LEGISLATION: Access and Aggregation: Public Records, Privacy and the Constitution, 86 Minn. L. Rev. 1137, 1139-40 (2002).

We then balance this privacy interest against plaintiff's interest in the disclosure of SSNs. Plaintiff does not provide any significant countervailing interest in the disclosure of SSNs; rather, he argues that by reading an exception to disclosure of the SSNs into OPRA as "inimical to the public interest," the trial court "created a huge loophole and

virtually eliminated OPRA as an independent right of access to records." Moreover, plaintiff argues that there can be no "reasonable expectation of privacy" for "records whose very purpose is to give public notice of the records' contents."

The amicus argues that its interest in SSNs lies in the fact that, when there is a search, in the context of property transfers, for judgments against an individual with the same name as another, "the inclusion of the social security number in the judgment record is the only way to confirm that the judgments are against a person of a similar name." We disagree with both plaintiff and the amicus in the need to disclose the SSNs on the requested realty records.

When we undertake a Doe analysis in balancing the interest in disclosure against the privacy interest, we find that the significant privacy interest clearly outweighs the negligible public interest in disclosure of an individual's SSN to a commercial entity gathering information to compile a database for sale to other commercial entities for profit. First, we consider the type of records requested. Doe, supra, 142 N.J. at 88. Here, they include mortgages, assignments of mortgages, deeds, lis pendens, and institutional liens. Second, we consider the information contained in the records. Ibid. Similar to the records requested in Doe, these records reveal

more than an individual's SSN; they also reveal the individual's name, marital status, home address, bank or mortgage holder and a specimen of his or her signature.

The third and fourth factors under the Doe analysis -- the potential for harm if the SSNs are released and "the injury from disclosure," ibid., -- are addressed in reports issued by the Government Accountability Office (GAO), the Federal Trade Commission (FTC), as well as the cases previously discussed herein.

Concerns about the use of SSNs and other personal information that could be used to commit fraud and identity theft "were heightened [in 2006] when an Ohio woman pled guilty to conspiracy, bank fraud, and aggravated identity theft as the leader of a group that stole citizens' personal identifying information from a local public record keeper's Web site and other sources, resulting in over \$450,000 in losses." U.S. Gov't Accountability Office, Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, though Other Vulnerabilities Remain, GAO-07-752, 1 (June 2007) (GAO Report).

The GAO concluded in its report that "the continued availability of social security numbers in public records, as well as increased access to these records through bulk sales and

Internet access, create the potential for identity theft." Id. at 11. "Social Security Numbers are . . . a key piece of information used to create false identities for financial misuse or [to] assume another individual's identity." Id. at 14. In 2005 alone, "approximately 8.3 million U.S. adults discovered that they were victims of some form of [identity] theft."⁴ Federal Trade Commission, 2006 Identity Theft Survey Report 4 (Nov. 2007)(FTC Report).

Plaintiff contends that the realty records maintained by the County Clerk are intended to be notice to the public of property ownership, liens and mortgages. That is indeed the purpose of such records, but we are not convinced that SSNs are essential to the notice provided by these records. Names, addresses, lot and block numbers clearly identify the properties.

The need for SSNs expressed by the amicus, "to confirm . . . judgments," is not sufficiently compelling to warrant disclosure when we consider the 8.3 million cases of identity theft reported by the Federal Trade Commission in 2005. FTC

⁴ "Identity theft is defined both by statute (ID Theft Act, 18 U.S.C. § 1028(a)(7), 1029(e)) and by FTC rule (16 C.F.R. § 603.2); it includes the misuse or attempted misuse of any identifying information – such as the SSN, biometric data, or an existing credit card account number – to commit fraud." FTC Report, supra, at 4.

Report, supra, at 4. In New Jersey alone, over 14,000 victims reported an incident of either fraud or identity theft in 2005. FTC Report, Consumer Fraud and Identity Theft Complaint Data, 3 (January 2007). And these numbers represent only the reported cases. Moreover, the interests represented by the amicus, the title searchers, have ready access to the realty records maintained by every county clerk in the state. They will not, therefore, be deprived of access to SSNs merely because they are redacted from documents compiled by plaintiff in a convenient commercial database.

The fifth, sixth and seventh factors in the Doe analysis involve the consideration of safeguards preventing unauthorized disclosure, the need for access and whether an express statutory mandate or public policy toward access exists. Doe, supra, 142 N.J. at 88. We need not address unauthorized disclosure here. The need for access, however, is a significant factor in our balancing of interests. The county clerk is authorized by statute to record and maintain realty documents, including title to real estate, conveyances, releases, declarations of trust, leases for more than two years, assignments, mortgages, deeds, liens and other encumbrances affecting real property. See N.J.S.A. 46:16-1.

The recorded documents are intended to serve as "notice to all subsequent judgment creditors, purchasers and mortgagees of the execution of the deed or instrument so recorded and of the contents thereof." N.J.S.A. 46:21-1. Indeed, the recorded realty documents are routinely accessed by attorneys, title searchers, creditors and potential purchasers, among others, to determine the status of a property or a title holder. Nothing in the recording statutes, however, contemplates the wholesale copying of millions of documents by commercial entities gathering and compiling information in databases for resale to other commercial entities for profit. See Higg-A-Rella, supra, 141 N.J. at 44.

The mere fact that a SSN is contained in a publicly filed realty record does not destroy an individual's privacy interest in his or her SSN. See Doe, supra, 142 N.J. at 82-83 (noting that the inclusion of a person's home address with other identifying information implicates a privacy interest, even though it is otherwise publicly available). As in Data Tree, the information sought by plaintiff is for commercial purposes, not public notice. We agree with the Kansas Supreme Court that the public interest served "by releasing unredacted documents with social security numbers . . . [and] dates of births to a

data collection agency [intending] to sell this information for a profit is at best insignificant." 109 P.3d at 1238.

In sum, under the circumstances presented here, when we balance plaintiff's interests against those of the individuals whose SSNs are contained in the realty documents filed with the county clerk, the individuals' interests prevail.

We are convinced that the right of privacy under the New Jersey Constitution, as articulated by our Supreme Court in Doe, in conjunction with the statutes and cases discussed at length herein, establishes protection for New Jersey citizens from wholesale disclosure of SSNs through OPRA requests for masses of recorded realty documents.

II

Plaintiff next argues that the portion of the order requiring "watermarking" on each document will delay the copying and add to plaintiff's costs. Defendants maintain that plaintiff consented to the watermarking at oral argument and cannot now challenge it on appeal. We agree.

At oral argument on October 25, 2006, plaintiff stated he had "no objection" to a watermark reflecting the date of copying. Judge Moses indicated she would include the watermarking requirement in her final order, and that counsel for both parties "will confer as to the appropriate language so

that anybody who sees this document will know it's as of such and such a date."

Plaintiff's counsel stated on the record that he had no objection under OPRA to the watermarking as long as any of plaintiff's competitors were subject to the same requirement that they pay for date-of-copying watermarks. Defendants' counsel agreed. The discussion concluded as follows:

THE COURT: They will agree that any company or entity seeking documents from the County Clerk would be required to submit to a watermark as well.

[PLAINTIFF'S COUNSEL]: Very good, Your Honor.

THE COURT: So, that's ordered.

[PLAINTIFF'S COUNSEL]: Thank you.

Accordingly, in the order entered on December 4, 2006, Judge Moses directed defendants to submit a bid that included among other things, "the costs of printing the copying dates on each aforesaid requested copied document." With respect to the watermark, the order included the following paragraphs:

IT IS FURTHER ORDERED that all copies of produced documents shall indicate, in print, the date of copying on said documents. The copying dates shall be written as follows, "COPY, produced on MM/DD/YY";

IT IS FURTHER ORDERED, the Court has determined a separate consent order will not be required regarding "watermarkings." The

Court has made the final decision on this issue;

IT IS FURTHER ORDERED, that the insert of said copying dates shall be "watermarked." For purposes of this order "watermarked" shall mean that the inserted copying date will not be able to be altered or removed;

IT IS FURTHER ORDERED that the watermarked copying date shall be inserted diagonally on each document. The font of the watermark data shall not obscure the contents of the document and will be no larger than 12 point font in size

Between oral argument on October 25, 2006, and the date the order was entered on December 4, 2006, plaintiff sent two letters to the court indicating that the parties could not agree on the language in the proposed order regarding the watermarks.

In our review of the transcript of October 25, 2006, plaintiff clearly stated his consent to watermarking the documents as long as a similar requirement was imposed on all others requesting the same documents. The December 4 order merely clarifies the content of the watermark and does not alter the substance of plaintiff's agreement stated on the record. Moreover, as defendants aptly note, the watermark indicating the date the copy was made will serve as notice that the record is correct as of that date, but may have been amended at a later date; for example, when recorded mortgages are updated in margin

notes indicating release, subordination, assignment, discharge or cancellation.

None of the arguments raised by plaintiff on appeal of this issue were presented to the trial court. We will not, therefore, consider them. Nieder v. Royal Indem. Ins. Co., 62 N.J. 229, 234 (1973).

III

Plaintiff finally argues that the trial court erred in denying his application for counsel fees. He contends that the court failed to give a statement of reasons and improperly denied fees to him as a "prevailing party" under OPRA. Defendants respond that (1) plaintiff waived his claim to counsel fees by not requesting them at oral argument; and (2) plaintiff was not a "prevailing party."

While plaintiff asked for counsel fees in his complaint, he did not pursue the request at oral argument. Judge Moses, sua sponte, said that she was "not giving" plaintiff counsel fees, unless "you give me a very good reason, which I haven't heard." Despite the judge giving plaintiff the opportunity to make his argument, he failed to do so. Nevertheless, plaintiff now maintains that he did not waive the claim. Rather, he states that once the judge denied counsel fees, any further argument on the issue "would have been futile" or would have subjected him

to "sanctions for unnecessary litigation under R. 1:4-8(a)(1)." Plaintiff's position on this issue is completely lacking merit in light of the judge's express invitation for him to persuade her otherwise. R. 2:11-3(e)(1)(E). Nevertheless, we add the following comment.

OPRA authorizes counsel fees to the "prevailing party" in any proceeding challenging a denial of access. N.J.S.A. 47:1A-6. In Teeters v. DYFS, 387 N.J. Super. 423, 431 (App. Div. 2006), certif. denied, 189 N.J. 426 (2007), we articulated a test for whether a party requesting fees under OPRA qualifies as a "prevailing party." The inquiry is whether the proceeding initiated by the plaintiff modified the public agency's behavior in a way that directly benefited the plaintiff. Id. at 432-33.

Plaintiff maintains that he "won the principal goal of his lawsuit: a court order requiring the City [sic] defendants to inform him of the fee for the copying requested." That, however, was only one of the issues before the court. In fact, the court's ruling, which we affirm in its entirety, rendered plaintiff a non-prevailing party with respect to most of the issues raised by him in the order to show cause. As Judge Moses noted, the gravamen of plaintiff's application was the redaction of SSNs. Accordingly, we are satisfied that, under the

circumstances presented here, the trial court properly denied
counsel fees.

Affirmed.

I hereby certify that the foregoing
is a true copy of the original on
file in my office.


CLERK OF THE APPELLATE DIVISION