

**NOT FOR PUBLICATION WITHOUT THE
APPROVAL OF THE APPELLATE DIVISION**

This opinion shall not "constitute precedent or be binding upon any court."
Although it is posted on the internet, this opinion is binding only on the
parties in the case and its use in other cases is limited. R. 1:36-3.

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-4665-14T4

STATE OF NEW JERSEY,

Plaintiff-Respondent,

v.

J.S.G.,¹

Defendant-Appellant.

Argued September 14, 2017 – Decided July 24, 2018

Before Judges Simonelli, Haas and Rothstadt.

On appeal from Superior Court of New Jersey,
Law Division, Gloucester County, Indictment
No. 13-12-1208.

Daniel S. Rockoff, Assistant Deputy Public
Defender, argued the cause for appellant
(Joseph E. Krakora, Public Defender, attorney;
Daniel S. Rockoff, of counsel and on the
briefs).

Steven A. Yomtov, Deputy Attorney General,
argued the cause for respondent (Christopher
S. Porrino, Attorney General, attorney; Steven
A. Yomtov, of counsel and on the brief).

¹ We use initials to identify those individuals involved in this
matter pursuant to Rule 1:38-3.

PER CURIAM

This appeal involves the warrantless, nonconsensual search of children's school records for the name of their father, defendant J.S.G., who was the owner of a vehicle linked to two burglaries. Defendant pled guilty to fourth-degree receiving stolen property, N.J.S.A. 2C:20-7, after the trial court denied his motion to suppress, and was sentenced to a two-year probationary term. We affirm the denial of the motion, but for different reasons than the court expressed in its February 25, 2015 oral opinion. Aquilio v. Cont'l Ins. Co. of N.J., 310 N.J. Super. 558, 561 (App. Div. 1998).

I.

The parties stipulated to the following facts at the suppression hearing. On August 18, 2013, a Westville police officer responded to a reported burglary at a home located on Magnolia Street. The homeowner informed Meyers that someone broke into his home and stole numerous household appliances and tools valued at approximately \$4000. There were no leads developed at the scene.

On August 28, 2013, a Westville police officer responded to a reported burglary at another home located on Magnolia Street. An electrician working at the home reported that several

appliances valued at approximately \$3000 were missing. The police found tire tracks leading from the driveway to the back door of the home that appeared to be wide enough to belong to a large pickup truck. There were no leads developed at the scene.

Westville Police Detective Donald Kiermeier, who was assigned to investigate both burglaries, obtained video surveillance from a building adjacent to the home burglarized on August 28, 2013. The video from one camera showed a pickup truck with five orange lights on the front of the cab driving away from the property, but did not show the driver or license plate number. The vehicle resembled an older two-tone red and silver pickup truck consistent with a 1980's Ford pickup truck (the truck). As the truck backed out of the driveway, it appeared to have items in the bed that were consistent with the appliances stolen from the home. A video from another camera also showed items in the bed that appeared to be appliances.

Kiermeier spoke to residents of Magnolia Street about the burglaries. Based on his description of the truck, a resident said he saw a similar truck frequently parked at another home on Magnolia Street and provided a photo of the truck from his home surveillance system. Kiermeier went to the home the resident identified and spoke to its occupant, L.H., who said the truck was often parked there and belonged to her children's father.

L.H. denied knowing about the recent burglaries on Magnolia Street and declined to give Kiermeier any information about him.

While speaking to L.H., Kiermeier noticed she had a child who appeared to be approximately seven years old. He contacted the principal of a local elementary school and asked if she was familiar with L.H. The principal said L.H. had two children enrolled at the school. Kiermeier obtained parental contact information from the principal, which listed defendant as the father. Kiermeier conducted a motor vehicle search and discovered defendant had a red Ford pickup truck registered in his name.

Kiermeier then went to Camden Iron & Metal, Inc. to determine whether defendant had scrapped any of the stolen items there. He obtained receipts for and photographs of items defendant had scrapped, which appeared to match the items stolen on August 18, 2013. He also obtained photographs of the truck, which showed the stolen items in the bed. He spoke to the victim, who positively identified the items shown in the photographs as his stolen property. Defendant was arrested the next day.

On his motion to suppress, defendant argued he had reasonable expectation of privacy in personally identifiable information (his name) contained in his children's school records because the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, and its corresponding regulation, 34 C.F.R. § 99, and the

New Jersey Pupil Records Act (NJPRA), N.J.S.A. 18A:36-19, and its corresponding regulations, N.J.A.C. 6A:32-7.1 to -7.8, guarantee parents the right to safeguard that information from improper disclosure.

The court found an individual ordinarily surrenders a reasonable expectation of privacy in information revealed to a third party and that "a person's name could hardly be thought of as protected privacy information." The court also found the policy behind FERPA and the NJPRA is to protect the student's privacy, not the privacy of the parent's name, and any violation implicated the school, not the police. The court determined, that a parent's name could be disclosed under FERPA as "directory information." The court concluded that "no privacy interest was violated so as to require a warrant as to the parent's name" and "[n]o information on the student was used as part of this investigation in any event." The court also held, sua sponte, that the inevitable discovery doctrine applied.

On appeal, defendant raises the following contentions.

POINT I

A POLICE OFFICER'S WARRANTLESS, NONCONSENSUAL SEARCH OF CHILDRENS' SCHOOL RECORDS FOR PATERNITY INFORMATION PROTECTED FROM UNAUTHORIZED ACCESS BY THE PLAIN TEXT OF FEDERAL, STATE, AND LOCAL PRIVACY LAWS VIOLATED DEFENDANT'S REASONABLE EXPECTATION OF PRIVACY UNDER THE FEDERAL AND STATE

CONSTITUTIONS [U.S. CONST., AMEND. IV; N.J. CONST., ART. I, ¶ 7].

A. Federal, State, And Local Privacy Laws Reflect A Broad Societal Consensus: [Defendant] Had A Reasonable Expectation Of Privacy In His Children's School Records And The Personally Identifying Information Therein, Including Paternity Information.

1. Federal Law Specifically Defines Paternity Information In School Records As "Personally Identifiable Information," Protected From Warrantless Disclosure Without Written Parental Consent.

2. While Federal Law Allows Local Authorities To Designate, By Public Notice, Categories Of "Personally Identifiable Information" That May Be Disclosed Without The Written Parental Consent Requirement ("Directory Information"), The State Offered No Proof That [The Children's Elementary School] Has Exempted Paternity Information In This Manner. If The State Had Looked, It Would Have Discovered That [The School's] Public Notice Actually Does Not Exempt Paternity Information From The Written Parental Consent Requirement.

3. Federal Law Prohibits Members Of The Public From Using A Mother's Name To Search School Records In Order To Learn The Names Of Her Children, And Any Paternity Information Associated With Those Children, Which Is Exactly What The Police Officer Did.

4. New Jersey State Law Did Not Permit The Officer's Warrantless, Nonconsensual Search. Federal Law Establishes A Privacy Floor Below Which State Law Cannot Sink.

5. Because The Plain Text of Federal, State, And Local Privacy Laws Clearly and Unambiguously Barred The Police Officer's Warrantless, Nonconsensual Search, The Court Had No Reason To Examine Statutory Purpose.

6. Although The Trial Court Had No Reason To Look Beyond The Clear And Unambiguous Plain Text Of Federal, State, And Local Privacy Laws, The Purpose Of These Laws Is Plainly To Protect Familial Privacy, Not Just The Privacy Of Children.

7. Leaving Aside FERPA's Federal, State, And Local Statutory Scheme Protecting A Right To Privacy In School Records, The New Jersey Supreme Court Has Also Found Constitutionally-Based Rights Protecting The Privacy Of Familial Associations And Consensual Adult Sexual Relationships.

B. The Trial Court Erred By Not Applying The Exclusionary Rule.

1. [Defendant] Did Not Waive His Reasonable Expectation Of Privacy In His Children's School Records And The Personally Identifying Information Therein.

2. The Trial Court Erroneously Applied The Inevitable Discovery Doctrine Sua Sponte, Without Any Explanation As To Why Or How The Evidence Would Have Been Inevitably Discovered, After The State Failed To Raise It Or Call Any Witnesses To Support It.

3. Because Federal, State, And Local Privacy Laws Explicitly Required The Police To Obtain A Judicial Search

Warrant, And The Police Did Not,
Exclusion Of The Evidence Here Would Only
Acknowledge The Social Choices Made By
The Political Branches.

Our Supreme Court has established the standard of review applicable to consideration of a trial judge's ruling on a motion to suppress:

We are bound to uphold a trial court's factual findings in a motion to suppress provided those "findings are supported by sufficient credible evidence in the record." Deference to those findings is particularly appropriate when the trial court has the "opportunity to hear and see the witnesses and to have the feel of the case, which a reviewing court cannot enjoy." Nevertheless, we are not required to accept findings that are "clearly mistaken" based on our independent review of the record. Moreover, we need not defer "to a trial . . . court's interpretation of the law" because "[l]egal issues are reviewed de novo."

[State v. Watts, 223 N.J. 503, 516 (2015)
(alteration in original) (citations
omitted).]

Because this appeal involves the court's interpretation of the law, our review is de novo with no deference afforded to the court's legal conclusions. Ibid.

II.

We first address defendant's argument that the court erroneously applied the inevitable discovery doctrine. The inevitable discovery doctrine is an exception to the exclusionary

rule. Nix v. Williams, 467 U.S. 431, 444 (1984). "If the State can show that 'the information ultimately or inevitably would have been discovered by lawful means . . . the deterrence rationale [of the exclusionary rule] has so little basis that the evidence should be received.'" State v. Maltese, 222 N.J. 525, 551-52 (2015) (alterations in original) (quoting Nix, 467 U.S. at 444).

In order to invoke the doctrine, the State must show by clear and convincing evidence that:

(1) proper, normal and specific investigatory procedures would have been pursued in order to complete the investigation of the case; (2) under all of the surrounding relevant circumstances the pursuit of those procedures would have inevitably resulted in discovery of the evidence; and (3) the discovery of the evidence through the use of such procedures would have occurred wholly independently of such evidence by unlawful means.

[State v. Keaton, 222 N.J. 438, 451 (2015) (quoting State v. Sugar, 100 N.J. 214, 238 (1985) (Sugar II)).]

The State must demonstrate that "had the illegality not occurred, it would have pursued established investigatory procedures that would have inevitably resulted in the discovery of the controverted evidence, wholly apart from its unlawful acquisition." Sugar II, 100 N.J. at 240. "[T]he central question to be addressed in invoking the 'inevitable discovery' rule 'is whether that very item of evidence would inevitably have been discovered, not merely

whether evidence roughly comparable would have been so discovered.'" State v. Worthy, 141 N.J. 368, 390 (1995) (citation omitted). However, "the State need not demonstrate the exact circumstances of the evidence's discovery It need only present facts sufficient to persuade the court, by a clear and convincing standard, that the [evidence] would be discovered." Maltese, 222 N.J. at 552 (alterations in original) (quoting State v. Sugar, 108 N.J. 151, 158 (1987) (Sugar III)).

Here, the State did not raise the inevitable discovery doctrine and presented no evidence, let alone clear and convincing evidence, satisfying the three requirements noted in Keaton. Accordingly, the court erred in speculating that the police would have inevitably discovered defendant's name. Nevertheless, defendant was not entitled to suppression of his name.

III.

Defendant contends that FERPA and the NJPRA create a reasonable expectation of privacy in his children's school records, including "personally identifiable information" (paternity information/his name) contained therein, and protect that information from disclosure under the Fourth Amendment and

Article 1, paragraph 7 of the New Jersey Constitution without a warrant or written parental consent.² We disagree.

FERPA and the Corresponding Regulations

FERPA governs the conditions for the availability of funds to educational agencies or institutions and the release of education records. See 20 U.S.C. § 1232g(a). FERPA provides that:

No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of educational records (or personally identifiable information contained therein other than directory information, as defined in [20 U.S.C. § 1232g(a)(5)] of students without the written consent of their parents to any individual, agency, or organization, other than [as stated in 20 U.S.C. § 1232g(b)(1)(A) to (L)].

[20 U.S.C. § 1232g(b)(1) (emphasis added).]

FERPA defines "directory information" as follows:

For the purposes of this section the term "directory information" relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous

² Post-argument, defendant cited to Brennan v. Bergen Cty. Prosecutor's Office, ___ N.J. ___ (2018) to support this argument. However, Brennan involved the Open Public Records Act, N.J.S.A. 47:1A-1 to -13, and has no bearing on the issues in this case.

educational agency or institution attended by the student.

[20 U.S.C. § 1232g(a)(5)(A) (emphasis added).]

The corresponding regulation, 34 C.F.R. § 99.3, defines "directory information" as follows, in pertinent part:

Directory information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.

(a) Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.

[(Emphasis added).]

FERPA has a public notice requirement for the disclosure of "directory information":

Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as such information with respect to each student attending the institution or agency and shall allow a reasonable period of time after such notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without the parent's prior consent.

[20 U.S.C. § 1232g(a)(5)(B) (emphasis added).]

The regulations also have a public notice requirement for the disclosure of "directory information":

An educational agency or institution may disclose directory information if it has given public notice to parents of students in attendance and eligible students in attendance at the agency or institution of:

(1) The types of personally identifiable information that the agency or institution has designated as directory information;

(2) A parent's or eligible student's right to refuse to let the agency or institution designate any or all of those types of information about the student as directory information; and

(3) The period of time within which a parent or eligible student has to notify the agency or institution in writing that he or she does not want any or all of those types of information about the student designated as directory information.

[34 C.F.R. § 99.37(a) (emphasis added).]

Here, the State argues that the name of a student's parent is included as "directory information" because the definition of "directory information" "includes, but is not limited to, the student's name." 33 C.F.R. § 99.3. However, the definition of "personally identifiable information" specifically includes "the name of the student's parent or other family members." Ibid. "Personally identifiable information" cannot be disclosed without

written parental consent unless the educational agency or institution designates it as "directory information" as described in 34 C.F.R. § 99.37. 20 U.S.C. § 1232g(b)(1); 34 C.F.R. §§ 99.30(a) and 99.31(a)(11).

In this case, the school district's public notice advised that the district must obtain written parental consent prior to the disclosure of "personally identifiable information." The public notice also advised that the district "may disclose appropriately designated 'directory information' without written consent, unless [the parent has] advised the [d]istrict to the contrary in accordance with [d]istrict procedures." The public notice did not designate the name of the student's parent as "directory information." Thus, parental consent was required before the disclosure of defendant's name under FERPA.

Nevertheless, defendant was not entitled to suppression of his name. FERPA is a funding statute with corresponding regulations establishing procedures for administrative enforcement and administrative remedies for improper disclosure of student records. See 20 U.S.C. § 1232g(f) and (g); 34 C.F.R. §§ 99.60(a) and (b), 99.63, 99.64(a) and (b), 99.65(a), 99.66(b) and (c)(1); and 99.67(1), (2) and (3). As we have made clear, "FERPA does not itself establish procedures for disclosure of school records. Rather, it provides that federal school funds will be withheld

from any school that effectively [violates FERPA] . . . and it requires educational agencies or institutions to establish appropriate procedures for granting access to such records to parents of school children." K.L. v. Evesham Twp. Bd. of Educ., 423 N.J. Super. 337, 363 (App. Div. 2011) (citation omitted). In addition, the United States Supreme Court has held that "FERPA's nondisclosure provisions further speak only in terms of institutional policy and practice, not individual instances of disclosure." Gonzaga Univ. v. Doe, 536 U.S. 273, 288 (2002) (emphasis added) (citing 20 U.S.C. § 1232b(b)(1) to (2) (prohibiting funding of "any educational agency or institution which has a policy or practice of permitting the release of education records")). What occurred here was an individual instance of disclosure.

More importantly, FERPA does not confer an enforceable right or provide for suppression in the event of a violation. As the Supreme Court made clear:

There is no question that FERPA's nondisclosure provisions fail to confer enforceable rights. To begin with, the provisions entirely lack the sort of "rights-creating" language critical to showing the requisite congressional intent to create new rights. Unlike the individually focused terminology of Titles VI and IX ("no person shall be subjected to discrimination"), FERPA's provisions speak only to the Secretary of Education, directing that "no funds shall

be made available" to any "educational agency or institution" which has a prohibited "policy or practice." 20 [U.S.C.] § 1232g(b)(1). This focus is two steps removed from the interests of individual students and parents and clearly does not confer the sort of "individual entitlement" that is enforceable under [42 U.S.C.] § 1983.

[Id. at 287 (citation omitted).]

See also Alexander v. Sandoval, 532 U.S. 275, 289 (2001) ("Statutes that focus on the person regulated rather than the individuals protected create 'no implication of an intent to confer rights on a particular class of persons'"). The Supreme Court held:

Our conclusion that FERPA's nondisclosure provisions fail to confer enforceable rights is buttressed by the mechanism that Congress chose to provide for enforcing those provisions. Congress expressly authorized the Secretary of Education to "deal with violations" of the Act, and required the Secretary to "establish or designate [a] review board" for investigating and adjudicating such violations. Pursuant to these provisions, the Secretary created the Family Policy Compliance Office (FPCO) "to act as the Review Board required under the Act and to enforce the Act with respect to all applicable programs." The FPCO permits students and parents who suspect a violation of the Act to file individual written complaints. If a complaint is timely and contains required information, the FPCO will initiate an investigation, notify the educational institution of the charge, and request a written response. If a violation is found, the FPCO distributes a notice of factual findings and a "statement of the specific steps that the agency or institution must take to comply" with FERPA. These

administrative procedures . . . further counsel against our finding a congressional intent to create individually enforceable private rights[.]

[Gonzaga Univ., 536 U.S. at 289-290 (emphasis added) (citations omitted).]

With a person having no enforceable private right under FERPA for a school's improper disclosure of "directory information" or "personally identifiable information," it logically follows that a person would also have no enforceable Fourth Amendment right for a school's improper disclosure of the name of a student's parent contained school records.

We elaborate this point in an analogous federal statute, the Federal Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2701 to 2712, which our Supreme Court has interpreted to confer no Fourth Amendment privacy interests. See State v. Evers, 175 N.J. 355, 372-73 (2003). The ECPA provides procedures by which a government entity may acquire subscriber information from an Internet service provider. 18 U.S.C. § 2703(c). "The ECPA requires a government entity seeking to procure subscriber information from an Internet service provider must do so by warrant, court order, subpoena, or consent of the subscriber." Evers, 175 N.J. at 372 (citing 18 U.S.C. § 270(c)(1)). "Although 18 U.S.C. § 2703 provides statutory privacy rights for Internet service provider subscribers, it does not afford an objectively

reasonable expectation of privacy under the Fourth Amendment."

Evers, 175 N.J. at 372-373 (2001). As the Court held:

Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their [internet service providers] retain, the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of "reasonably objective" for Fourth Amendment purposes. Despite its concern for privacy, Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act For Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of [i]nternet connection. The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information.

[Id. at 374 (emphasis added) (citation omitted).]

We follow the holdings in Gonzaga Univ. and Evers that FERPA does not create an objectively reasonable expectation of privacy in student records recognized by the Fourth Amendment. Accordingly, defendant had no reasonable expectation of privacy in his children's school records, including the paternity information contained therein, and was not entitled to suppression of his name.

The NJPRA and the Corresponding Regulations

The NJPRA requires the State Board of Education to:

provide by regulation for the creation, maintenance and retention of pupil records and for the security thereof and access thereto, to provide general protection for the right of the pupil to be supplied with necessary information about herself or himself, the right of the parent or guardian and the adult pupil to be supplied with full information about the pupil, except as may be inconsistent with reasonable protection of the persons involved, the right of both pupil and parent or guardian to reasonable privacy as against other persons and the opportunity for the public schools to have the data necessary to provide a thorough and efficient educational system for all pupils.

[N.J.S.A. 18A:36-19.]

The corresponding regulation, N.J.A.C. 6A:32-7.1(b), requires school districts to "compile and maintain student records and regulate access, disclosure, or communication of information contained in educational records in a manner that assures the security of such records in accordance with this subchapter."

In addition to these requirements, N.J.A.C. 6A:32-7.1(g)(5) requires school districts to "establish written policies and procedures for student records that . . . [a]llow for release of school contact directory information for official use, as denied by N.J.A.C. 6A:32-7.2." "Student record" is defined as:

information related to an individual student gathered within or outside the school district

and maintained within the school district, regardless of the physical form in which it is maintained. Essential in this definition is the idea that any information that is maintained for the purpose of second-party review is considered a student record. Therefore, information recorded by certified school personnel solely as a memory aid and not for the use of a second party is excluded from this definition.

[N.J.A.C. 6A:32-2.1.]

Mandated student records that school districts must maintain include "[t]he student's name, address, telephone number, date of birth, name of parent(s), gender, standardized assessment results, grades, attendance, classes attended, grade level completed, year completed, and years of attendance[,]" and "[a]ll other records required by N.J.A.C. 6A." N.J.A.C. 6A:32-7.3.

N.J.A.C. 6A:32-7.5(a) provides that "[o]nly authorized organizations, agencies or persons as defined in this section shall have access to student records, including student health records." N.J.A.C. 6A:32-7.5(e) lists the authorized organizations, agencies, and persons permitted access to "student records." The list does not include law enforcement.

In addition to "student records," school districts must "compile and maintain a school contact directory for official use that is separate and distinct from the student information directory." N.J.A.C. 6A:32-7.2(a); see also N.J.A.C. 6A:32-7.3

(requiring school districts to maintain "[a]ll other records required by N.J.A.C. 6A").

N.J.A.C. 6A:32-2.1 defines "school contact directory for official use" as "a compilation by a district board of education that includes the following information for each student: name, address, telephone number, date of birth and school of enrollment. The directory may be provided for official use only to judicial, law enforcement, and medical personnel." (Emphasis added).

N.J.A.C. 6A:32-7.2(a) requires school districts to:

provide information from the school contact directory for official use only to judicial and law enforcement personnel, and to medical personnel currently providing services to the student in question. Upon request from a court, other judicial agency, law enforcement agency, or medical service provider currently providing services to the student in question, school personnel shall promptly verify the enrollment of a student and provide the requester with all information about the student that is contained in the school contact directory for official use.

[(Emphasis added).]

N.J.A.C. 6A:32-2.1 defines "student information directory" as:

a publication of a district board of education that includes the following information relating to a student. . . .

1. Name;
2. Grade level;
3. Date and place of birth;

4. Dates of school attendance;
5. Major field of study;
6. Participation in officially recognized activities;
7. Weight and height relating to athletic team membership;
8. Degrees;
9. Awards;
10. The most recent educational agency attended by the student; and
11. Other similar information.

[(Emphasis added).]

N.J.A.C. 6A:32-2.1 further provides that information from a "student information directory" "shall be used only by authorized school district personnel and for designated official use by judicial, law enforcement, and medical personnel and not for general public consumption." Ibid. (emphasis added).

Putting this all together, although not explicitly stated in the regulations, a "student information directory," which "shall be used only by . . . law enforcement," could include as "[o]ther similar information" the name of a student's parent. N.J.A.C. 6A:32-2.1. Similarly, a "school contact directory for official use," which must be provided to law enforcement upon request, could include the name of a student's parent. Defendant's name came from the school's parental contact information, and thus, could be disclosed to law enforcement without written parental consent.

In any event, since a student's name can be disclosed to law enforcement, N.J.A.C. 6A:32-2.1, and must be disclosed to law enforcement upon request, N.J.A.C. 6A:32-7.2(a), it would be incongruous for the name of a student's parent's to garner any greater privacy protection than their child's name. Accordingly, there was no violation of the NJPRA or its governing regulations here.

Even if there was a violation, this did not entitle defendant to suppression of his name. Like FERPA, the NJPRA and its governing regulations merely provide administrative remedies for a violation and do not provide for a private right of action or suppression. L.S. and R.S. v. Mount Olive Bd. of Educ., 765 F. Supp. 2d 648, 664 (D.N.J. 2011) (holding that FERPA and the NJPRA do not provide a private right of action); see also N.J.A.C. 6A:32-7.7 (administrative remedies).

We conclude that the NJPRA does not create an objectively reasonable expectation of privacy in student records recognized by the Fourth Amendment or Article 1, paragraph 7 of the New Jersey Constitution. Accordingly, defendant had no reasonable expectation of privacy in his children's school records, including the paternity information contained therein, and was not entitled to suppression of his name.

IV.

Defendant contends the motion judge erred by not applying the exclusionary rule. He argues that aside from FERPA and the NJPRA, he had a reasonable expectation of privacy in the paternity information (his name) contained in his children's school records, and argues he did not waive that right by giving his name to the school. The State counters that a person has no reasonable expectation of privacy in his or her name, and even if there was a privacy right, one's identity cannot be suppressed from criminal prosecution as a matter of law. We agree with the State.

"To invoke the protections of the Fourth Amendment and its New Jersey counterpart, Article I, Paragraph 7, defendant must show that a reasonable or legitimate expectation of privacy was trammelled by government authorities." Evers, 175 N.J. at 355, 369. "To meet this test, [the defendant] must establish that he had both 'an actual (subjective) expectation of privacy,' and 'one that society is prepared to recognize as reasonable.'" Id. at 369 (citations omitted).

"It has long been accepted that '[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'" Ibid. (citations omitted). "An individual ordinarily surrenders a reasonable expectation of privacy to information revealed to a third-party. If that third-party

discloses the information to the government, the individual, who falsely believed his confidence would be maintained, will generally have no Fourth Amendment claim." Ibid. (citations omitted).

In addition, a person "cannot have a reasonable expectation of privacy" in information "readily available through public records," including a person's name. Doe v. Poritz, 142 N.J. 1, 80 (1995). However, although information "may be available to the public, in some form or other, [that] does not mean [a person] has no interest in limiting its dissemination." Burnett v. Cty. of Bergen, 198 N.J. 408, 430 (2009) (citation omitted). When such information is "combined with other personal information" it may "elevate[] the privacy concern at stake." Id. at 430. It is only when information, e.g., a person's name, along with personal identifiers, are collectively assembled that protected privacy interests are implicated. See id. at 430-31; Poritz, 198 N.J. at 81-82. For example, New Jersey recognizes a reasonable expectation of privacy in the following records that have information combined with other personal information: subscriber information an individual provides to an Internet service provider, State v. Reid, 194 N.J. 386, 399 (2008); utility records, State v. Domicz, 188 N.J. 285, 299 (2006); bank records, State v. McAllister, 184 N.J. at 17, 31 (2005); and telephone toll-billing, State v. Hunt,

91 N.J. 338, 347-48 (1982).

However, New Jersey has not recognized a reasonable expectation of privacy in a phone number. State v. DeFranco, 426 N.J. Super. 240, 248-50 (App. Div. 2012). In DeFranco, the police were investigating the defendant for his alleged sexual assault of a student and obtained his cell phone number from the school to conduct a consensual telephone intercept between him and the victim. Id. at 243-44. We disagreed with the defendant that his cell phone number should be afforded the same protection as in Reid, Domicz, McAllister and Hunt. Id. at 248. "We perceive[d] a significant difference between the 'generated information'[³] afforded protection by the New Jersey Supreme Court in its privacy decisions and the 'assigned information that defendant seeks to protect in this case.'" Id. at 249. We found that:

The [Internet service provider] records, the long-distance billing information, the banking records, and the utility usage records of Reid, Hunt, McAllister, and Domicz, respectively, constituted the keys to the details of the lives of those to which the seemingly innocuous initial information pertained. While in some circumstances, knowledge of a telephone number might be equally revelatory, here it was not. The number was simply a number. In the

³ Generated information refers to financial information such as credit card records, medical records, and phone logs; assigned information includes name, address, and social security number. DeFranco, 426 N.J. Super. at 249 (citation omitted).

circumstances of this case, we do not find that defendant's professed subjective expectation of privacy is one that society would be willing to recognize as reasonable.

[Id. at 249-50 (emphasis added) (citations omitted).]

We also determined that even if the defendant had a protectable privacy interest in his cell phone number, he waived that interest by disclosing the number to third-parties and including it in the school's staff directory. Id. at 250.

Here, defendant had no reasonable expectation of privacy in his name contained in his children's school records. The police simply obtained his name from the school's parental contact information and no other records, personal identifiers, information, or details of his life that would implicate constitutionally protected privacy interests. Defendant's name, by itself, did not touch upon matters that a reasonable person would deem private. Since defendant has no privacy interest in his name, the exclusionary rule did not apply.

Regardless of any expectation of privacy in a person's name, a defendant's identity cannot be suppressed based on a purported violation under either the Fourth Amendment or Article 1, paragraph 7 of the New Jersey Constitution. The Supreme Court has held that the exclusionary rule only applies to the fruits of a constitutional violation, such as tangible, physical evidence

seized, items observed or words overheard, or confessions or statements of the accused. United States v. Crews, 445 U.S. 463, 470 (1980). The exclusionary rule does not apply to a person's identity. As the United States Supreme Court has held:

[a]sking questions is an essential part of police investigations. In the ordinary course a police officer is free to ask a person for identification without implicating the Fourth Amendment. "[I]nterrogation relating to one's identity or a request for identification by the police does not, by itself, constitute a Fourth Amendment seizure."

[Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 185 (2004) (quoting INS v. Delgado, 466 U.S. 210, 216 (1984)).]

The Supreme Court has also held that a defendant's identity "is never itself suppressible as a fruit of an unlawful arrest, even if it is conceded that an unlawful arrest, search, or interrogation occurred." INS v. Lopez-Mendoza, 468 U.S. 1032, 1039-40 (1984). The Supreme Court did not consider "egregious violations of Fourth Amendment or other liberties that might transgress notions of fundamental fairness and undermine the probative value of the evidence obtained." Id. at 1050-51.

In United States v. Farias-Gonzales, 556 F.3d 1181 (11th Cir. 2009), the Eleventh Circuit weighed the heavy social costs of suppressing identity evidence and concluded that evidence "offered solely to prove the identity of [a] defendant" was admissible. Id.

at 1187, 1189. The court explained that in Hiibel, the Supreme Court stated:

"[i]n every criminal case, it is known and must be known who has been arrested and who is being tried." Both the court and the Government are entitled to know who the defendant is, since permitting a defendant to hide who he is would undermine the administration of the criminal justice system. For example, a defendant who successfully suppressed all evidence of his identity could preclude consideration of his criminal history, which could give rise to relevant and admissible evidence at trial.

. . .

The Constitution does not prohibit the Government from requiring a person to identi[f]y himself to a police officer.

[Id. at 1187-88 (citations omitted).]

The Farias-Gonzales court further explained:

Additionally, even if a defendant in a criminal prosecution successfully suppresses all evidence of his identity and the charges are dropped, the Government can collect new, admissible evidence of identity and re-indict him. This is so because identity-related evidence is not unique evidence that, once suppressed, cannot be obtained by other means. The application of the exclusionary rule to identity-related evidence will have a minimal deterrence benefit, as its true effect will often be merely to postpone a criminal prosecution.

[Id. at 1188-89 (citation omitted).]

See also Reid, 194 N.J. at 406 (finding suppression of the Internet

service provider records did "not mean that the evidence is lost in its entirety[,]" as the records "existed independently of the faulty process the police followed" and could be "reliably reproduced and lawfully reacquired through a proper grand jury subpoena").

We are not concerned here with any egregious violations. All the police did was obtain defendant's identity through the school's parental contact information and no other evidence. Defendant's identity itself, even if it was obtained by an unlawful search, was not suppressible under the exclusionary rule.

Lopez-Mendoza, 468 U.S. at 1039-40.

Affirmed.

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



CLERK OF THE APPELLATE DIVISION