SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF ALBANY

JAMES SHULTZ and RENEE CHEATHAM,

Petitioners,

-against-

NEW YORK STATE EDUCATION DEPARTMENT, SHANNON TAHOE, in her official capacity as Interim Commissioner of Education of the New York State Education Department, and TEMITOPE AKINYEMI, in her official capacity as Chief Privacy Officer of the New York State Education Department,

Respondents,

For a Judgment Pursuant to Article 78 of the Civil Practice Law and Rules

Index No. _____

VERIFIED PETITION

ORAL ARGUMENT REQUESTED

Petitioners, James Shultz and Renee Cheatham by and through their attorneys, the New York Civil Liberties Union Foundation, allege as follows:

PRELIMINARY STATEMENT

1. This Article 78 proceeding challenges the determination by the New York State Education Department ("NYSED") that a biometric face recognition technology system in the Lockport City School District ("Lockport" or the "District") that scans each student's face every time they walk by one of the system's 300 high resolution surveillance cameras in order to take biometric measurements of the student's face does not implicate "student data" under New York's Education Law.

2. Lockport activated a biometric face recognition technology system in all of its schools, from elementary to high school on January 2, 2020. The Lockport face recognition system scans and takes biometric measurements of the face of each student—kindergartener and

high school senior alike—every time they walk by one of the 300 high-resolution surveillance cameras installed throughout Lockport's eight schools.

3. This intrusive and inaccurate system has been deployed on children because NYSED erroneously found that the system does not implicate "student data" as defined under New York's Education Law § 2-d, thus depriving Lockport's students of the law's vital privacy protections.

4. Yet the Lockport face recognition system engages in real-time collection, analysis, and retention of biometric information from each child in Lockport's schools. Face recognition technology attempts to recognize and identify a human face through the automated, computational analysis of their facial features. Face recognition software, as used in the Lockport system, first analyzes video camera footage for the appearance of any faces, and then further analyzes each face by its features to create a biometric template, or unique facial signature, that represents the individual. Each biometric template is then compared to stored biometric samples in the system's database for any statistical matches.

5. Education Law § 2-d is intended to protect student privacy and thus affords a high degree of security to the personally identifiable information ("PII") of students, as that term is defined in the federal Family Educational Rights and Privacy Act ("FERPA"), 12 U.S.C. §1232g, and accompanying regulations, 34 C.F.R. § 99.3. The definition of student PII explicitly includes students' biometric information. However, Respondents mistakenly determined that the Lockport face recognition system does not implicate student data and, consequently, none of the protections and requirements of Education Law § 2-d protect the PII of students that is continuously captured by the system.

6. NYSED articulated this flawed finding in a letter to Lockport dated November 27,

2019, in which it gave permission for Lockport to begin using the face recognition system (the "Determination"). Affidavit of Stefanie D. Coyle, dated June 9, 2020 ("Coyle Aff.") Ex. 1. The Determination was an abrupt reversal of NYSED's previous position. In the 18 months prior to that date, NYSED engaged extensively with Lockport to secure students' biometric information: NYSED required Lockport to undertake a privacy assessment; reviewed Lockport's draft privacy policies; and even told the public that it would "ensure that student data will be protected with the addition of the new technology." Coyle Aff. Exs. 5-9, 11-15, 17.

7. In June 2019 and then again in September 2019, NYSED explicitly prohibited Lockport from testing its face recognition technology. As late as October 2019, NYSED stated that it was still continuing "to research and review" the issue of the use of biometric surveillance in schools. Coyle Aff. Ex. 18. Yet on November 27, 2019, NYSED made an inexplicable about-face in its determination that Lockport's system did not implicate student data – even though none of the underlying facts had changed.

8. NYSED appears to have based its reversal and the decision to allow the system to operate on the mere fact that Lockport agreed to remove any students from its reference database, the so-called "Hot List." Coyle Aff. Ex. 20.

9. NYSED's Determination reflects a fundamental misunderstanding of how face recognition technology works and is contrary to the plain language of state and federal laws that govern the confidentiality of education records.

10. NYSED's arbitrary, capricious, and irrational Determination that Lockport's face recognition system does not involve the creation or maintenance of student data endangers Lockport's students and parents by stripping them of the heightened protections of Education Law § 2-d for this sensitive biometric information. It leaves students and parents without any

recourse when the Lockport face recognition systems suffers a breach or should Lockport's vendors seek to use this data for commercial purposes.

11. The Respondents' Determination will lead to the intrusive and flawed collection of student biometric information without any benefit to Lockport's schools, students, or the community. Pursuant to Article 78, the court should annul the Respondents' Determination and restore the petitioners' privacy rights, including all of the protections and remedies guaranteed by Education Law § 2-d, relating to the personally identifiable biometric information of their children who attend school in the Lockport City School District.

VENUE

12. Pursuant to C.P.L.R. 7804(b) and 506(b), venue in this proceeding lies in Albany County, in the judicial district in which the Respondents took the action challenged here and where the office of the Respondents are located.

PARTIES

Petitioners

13. Petitioner Renee Cheatham is a resident of Lockport, New York. She is the parent of one student and the grandparent of three other students currently attending Lockport schools.

14. Petitioner James Shultz is a resident of Lockport, New York. He is the parent of a student currently attending Lockport schools.

Respondents

15. Respondent New York State Department of Education ("NYSED") is a New York State agency constituted under New York Education Law § 101. NYSED is "charged with the general management and supervision of all public schools and all of the educational work of the

state." N.Y. Educ. Law § 101. NYSED, through its employees, made the determination that the Lockport face recognition system does not implicate student data and, as a result, allowed Lockport to operate it. NYSED is a body within the meaning of Article 78 of the CPLR. NYSED maintains its office at 89 Washington Avenue, Albany, New York 12234.

16. Respondent Shannon Tahoe is NYSED's Interim Commissioner of Education. Pursuant to N.Y. Educ. Law § 305, Respondent Tahoe is charged to enforce all general and special laws relating to the educational system of the state and execute all educational policies determined upon by the Board of Regents. Respondent Tahoe is an officer within the meaning of Article 78 of the CPLR. Respondent Tahoe maintains an office at NYSED at 89 Washington Avenue, Albany, New York 12234. Respondent Tahoe is sued in her official capacity as Interim Commissioner of Education of the New York State Education Department.

17. Respondent Temitope Akinyemi is NYSED's Chief Privacy Officer. Respondent Akinyemi has oversight responsibilities delineated under Education Law § 2-d, including the obligation to review and comment upon any department program, proposal, grant, or contract that involves the processing of student data or teacher or principal data before the commissioner begins or awards the program, proposal, grant, or contract. Pursuant to Education Law § 2-d and the Part 121 Regulations, the Chief Privacy Officer "may require an educational agency to act to ensure that personally identifiable information is protected in accordance with state and federal law and regulations, including but not limited to requiring an educational agency to perform a privacy impact and security risk assessment." Upon information and belief, exercising her statutory and regulatory authority, Respondent Akinyemi required Lockport to conduct a privacy impact and security risk assessment of the Lockport face recognition technology system and reviewed Lockport's draft privacy policies relating to its face recognition technology system.

Respondent Akinyemi signed the November 27, 2019 Determination. Respondent Akinyemi is an officer within the meaning of Article 78 of the CPLR and maintains an office at NYSED at 89 Washington Avenue, Albany, New York 12234. Respondent Akinyemi is sued in her in her official capacity as Chief Privacy Officer of the New York State Education Department.

FACTS

Lockport's Acquisition of its Face Recognition System

18. In 2016, the Lockport City School District filed an application to use $3,810,833 of New York State Smart Schools Bond Act funds to acquire a face recognition system for all eight of its K-12 schools in the District.

19. NYSED, along with the New York State Budget Director and Chancellor of the State University of New York, who are the members of the Smart Schools Bond Act Review Board, approved Lockport's application.

20. Lockport did not engage parents, students, and teachers in the process by which the District acquired, installed and activated its face recognition system in all of Lockport's schools. Lockport held only one public meeting to introduce the community to the idea of using state money for technology in the classroom to purchase surveillance technology. That meeting was held on August 17, 2016, in the middle of a weekday afternoon in mid-August, when many parents were at work or out of town on summer vacation. Lockport sent no emails or flyers to students and parents during the process of acquiring and installing this technology in the District's schools. Affidavit of Renee Cheatham, dated June 9, 2020 ("Cheatham Aff.") ¶ 4.[1]

21. On March 28, 2018, Lockport's School Board voted to award a bid made by Ferguson Electric Construction Company ("Ferguson ECC") to install enhanced surveillance

[1] Lockport communicated with their students' families only after the system was fully installed and about to be activated. *See* Coyle Aff. Ex. 10.

cameras, as well as software and other hardware components for a face recognition system. Affidavit of Daniel Schwarz dated June 9, 2020 ("Schwarz Aff.") ¶ 11.

22. The Lockport face recognition system is called the "AEGIS" face recognition system. The AEGIS software technology is trademarked and marketed by SN Technologies Corp. based in Gananoque, Ontario, Canada ("SN Tech"). Schwarz Aff. ¶ 10.

23. Prior to providing the AEGIS system for Lockport, SN Tech had no experience whatsoever working with schools much less student data. Schwarz Aff. ¶¶ 5-6.

24. NYSED was aware that SN Tech had no experience whatsoever working with schools much less student data that is protected by Education Law §2-d. Schwarz Aff. ¶¶ 5-6; Coyle Aff. Ex. 21.

25. Ferguson ECC did not have any expertise in face recognition systems and admitted that it was completely dependent on the manufacturer's representations concerning privacy and security issues. Schwarz Aff. ¶¶ 5-6.

26. Ferguson ECC had no experience whatsoever handling student data that is protected by Education Law §2-d. Schwarz Aff. ¶¶ 5-6.

27. Upon information and belief, NYSED also was aware that Ferguson ECC had admitted publicly that it had no experience whatsoever with face recognition systems and was completely dependent on the manufacturer's representations concerning privacy and security issues. Schwarz Aff. ¶¶ 5-6, Ex. 3.

28. Lockport does not hold the contract for the AEGIS software directly with SN Tech. Schwarz Aff. ¶ 12.

29. Rather, Lockport awarded the contract for the surveillance camera system and the hardware and face recognition software to Ferguson ECC, which then purchased the face recognition system from SN Tech. Schwarz Aff. ¶¶ 10-13.

30. Lockport, upon information and belief, has no control over the AEGIS software system and has no ability to modify, direct, or enforce the terms and conditions of the AEGIS software technology contract. Schwarz Aff. ¶14.

31. NYSED was aware that Lockport appears to have structured its acquisition of the AEGIS face recognition system intentionally to avoid the strictures imposed on third-party contractors by Education Law § 2-d. Coyle Aff. Exs. 21-24, 26-31.

The Operation of Lockport's Face Recognition System

32. Face recognition technology is a way of recognizing, and identifying, a human face through the automated, computational analysis of its facial features. Face recognition software, as used by Lockport School District, first analyzes video camera footage for the appearance of any faces, which it then further analyzes by its features to create a biometric template that represents the individual. Each biometric template is then compared to stored biometric samples in the system's database for any statistical matches. The statistical threshold that constitutes a successful match depends on each system, implementation, and policy decision. Lockport has not released any of this information. Schwarz Aff. ¶ 17.

33. Lockport's face recognition system uses 300 closed-circuit cameras that are installed in all the public and common areas, such as building entrances, stairwells, hallways, cafeterias, parking lots, auditoriums, gymnasiums or playgrounds of all eight schools in the Lockport school district. Coyle Aff. Ex. 2; Schwarz Aff. ¶ 18.

34. The cameras constantly record the faces of all students who pass through or gather in the areas under surveillance. Schwarz Aff. ¶ 20.

35. All of the student facial images recorded by the surveillance cameras are continuously analyzed by the Lockport database system; the software reads the geometry of all faces and calculates whether those students' unique facial signatures match a "persons of interest" database—or a "Hot List"—which contains the photographs of unwanted persons. Schwarz Aff. ¶ 20.

36. The Lockport school administrators decide how to populate the persons of interest on the Hot List. Schwarz Aff. ¶ 20.

37. The persons of interest currently populating the Hot List include suspended staff and sex offenders, as well as "anyone prohibited from entry to District property by court order presented to the District" or "[a]nyone believed to pose a threat based on credible information presented to the District" and "[s]chool security and law enforcement personnel." Coyle Ex. 2. Schwarz Aff. ¶ 21.

38. In order for Lockport's system to determine whether there are any matches to the individuals on their persons of interest database, or Hot List, it has to analyze all faces that appear in the camera frames. Because every face that is detected in the frame will be analyzed and compared to entries on the Hot List, anyone who walks through areas captured by the surveillance cameras will be entered into the face recognition system, including students. Schwarz Aff. ¶ 22.

39. All surveillance camera footage is retained for a period of 60 days, if not longer at the District's discretion. Schwarz Aff. ¶ 22.

40. Privacy Policy 2020 5685 provides multiple exceptions allowing such data to be stored for longer periods of time. Schwarz Aff. ¶ 22.

41. Student biometric data is implicated whenever there is a misidentification that falsely matches a student to an individual in the database. Schwarz Aff. ¶ 23.

42. Lockport's privacy policy, 2020 5685, makes clear that misidentifications may occur and that certain data will be maintained in such instances. Schwarz Aff. ¶ 23.

NYSED's Exercise of Authority under Education Law § 2-d and the Part 121 Regulations relating to Lockport's Face Recognition System

43. As early as June 2018, and for a period of at least 18 months, NYSED properly understood that the Lockport face recognition system implicated the privacy and security of student data, as that term is defined in Education Law § 2-d.

44. Upon information and belief, NYSED directed Lockport to perform a risk assessment of its face recognition system on or after a telephone conversation with Lockport officials as early as June, 2018. Coyle Aff. Ex. 6. For the following period of 18 months, NYSED had to guide Lockport in addressing the privacy concerns raised by its own system.

45. Lockport submitted a risk assessment to NYSED by letter dated November 20, 2018. Coyle Aff. Ex. 5.

46. By letter dated December 6, 2018, NYSED informed Lockport that their risk assessment "does not sufficiently demonstrate an understanding of the risk factors that will be present when facial technology is implemented, and therefore does not thoroughly reflect that the steps taken to eliminate or mitigate such factors will be adequate. It was particularly concerning that the preparer of the report failed to grasp that student images on the district's servers are personally identifiable information." Coyle Aff. Ex. 6. NYSED followed up the December 6, 2018 letter with an email advising Lockport that "the District has not demonstrated that the

necessary framework (policies, procedures and technology) is in place to protect the privacy of data subjects and properly secure the data." Coyle Aff. Ex. 7.

47. As late as April 2019, almost one year into working to craft a privacy policy that complied with Education Law § 2-d, Lockport entered into a contract to outsource the monitoring of the face recognition system cameras to an unrelated third party. After NYSED expressed concerns about third-party vendors having access to private student and staff information, Lockport cancelled that third party contract. When asked to respond to NYSED's concerns about third-party vendors having access to private student information, Superintendent Bradley is reported to have stated: "Privacy matters are a big deal nowadays." Schwarz Aff. ¶5, Ex. 1.

New York Education Law § 2-d and the Part 121 Regulations

48. Education Law § 2-d imposes a variety of restrictions on how districts, schools and vendors can collect, use and disclose student data; the statute regulates the way schools and vendors must secure student data and imposes a complete ban on the sale of personal student information or its use for marketing and commercial purposes.

49. Education Law § 2-d defines "student data" as "personally identifiable information from student records of an educational agency." Education Law § 2-d(1)(i).

50. "'Personally identifiable information,' as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code ["FERPA" …]." Education Law § 2-d(1)(e).

51. 34 C.F.R. § 99.3 defines "personally identifiable information" to include "(d) A personal identifier, such as the student's . . . biometric record" and "(f) [o]ther information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty."

52. "Biometric record" as used in the FERPA definition of personally identifiable information, means "a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; face characteristics; and handwriting." 34 C.F.R. § 99.3.

53. Education Law § 2-d provides remedies for breaches the security and confidentiality of such data, including monetary fines.

54. Both Education Law § 2-d and the enabling regulations at 8 N.Y.C.R.R. Part 121 Regulations confer the Chief Privacy Officer with broad powers to "require an educational agency to act to ensure that [student] personally identified information is protected."

At All Times Prior to November 27, 2019, NYSED Understood that the Lockport Face Recognition System Implicated Student Data

55. Lockport installed its face recognition technology system in the summer of 2018 and had intended to utilize it at the start of the academic year that 2018. Coyle Aff. Ex. 3.

56. However, upon information and belief, in June 2018, NYSED intervened and requested that Lockport delay activating the system pending Lockport's conduct of a "privacy assessment of their proposed use of this technology to ensure that the district is in compliance with state and federal laws, and that students' personally identifiable information is properly protected." Coyle Aff. Ex. 6.

57. In directing Lockport to conduct this "privacy assessment," NYSED's Chief Privacy Officer exercised her power to require a school district to "perform a privacy impact and security risk assessment" in order to "ensure that [student] personally identifiable information is protected." Education Law § 2-d(2)(c); 8 N.Y.C.RR 121.13(b).

Lockport's Efforts to Draft a Privacy Policy to Ensure Student Data is Protected in Accord with Education Law § 2-d

58. As part of NYSED's requested privacy impact and security risk assessment of the Lockport face recognition system, Lockport issued several draft privacy policies governing the face recognition system before the Lockport Board of Education finally adopted Policy 2020 5685 on January 8, 2020. Coyle Aff. Exs. 2, 19.

59. Lockport's attempts at devising a privacy policy that complies with Education Law § 2-d, though ultimately unsuccessful, demonstrate that Lockport's biometric face recognition system creates and maintains student data as defined by that law.

Lockport's November 2018 Draft Privacy Policy

60. Lockport publicly issued its first draft privacy policy on Monday, November 5, 2018 (the "November 2018 privacy policy"), after months of pressure from Lockport parents, the advocacy community, and NYSED. Coyle Aff. Ex. 4.

61. The November 2018 privacy policy addressed a variety of matters including access to system hardware and the software databases, security alerts and responses, and length of retention of images collected from the schools' closed circuit surveillance cameras. Coyle Aff. Ex. 4.

62. The November 2018 privacy policy also identified that Lockport would place suspended students on the Hot List. Coyle Aff. Ex. 4.

63. The November 2018 privacy policy established no meaningful limits on

sharing information produced by the face recognition system with law enforcement or "other governmental authorities," such as U.S. Immigration and Customs Enforcement. Coyle Aff. Ex. 4.

64. The November 2018 policy demonstrated that the District had little understanding of the student privacy mandate of FERPA, which prohibits the sharing of certain information in education records without prior consent from a parent or eligible student except in enumerated, limited exceptions. Coyle Aff. Ex. 4.

65. Although the Lockport School Board voted to approve this policy in December 2018, NYSED did not approve the November 2018 draft policy and, upon information and belief, directed Lockport to undertake further revisions to the policy. Coyle Aff. Exs. 6, 7.

Lockport's August 2019 Draft Privacy Policy

66. During the late winter and spring of 2019, Lockport repeatedly announced that it intended to activate and test its face recognition system. Coyle Aff. Exs. 10-12.

67. NYSED, however, stated that it continued to have concerns with the privacy and security aspects of Lockport's face recognition system and announced publicly that it had not granted Lockport permission to utilize its technology. Coyle Aff. Ex. 12.

68. A NYSED spokesperson provided an extensive email statement to BuzzFeed News on May 30, 2019, specifically noting concerns about protection of "student data" within the system:

> The Department is currently reviewing the Lockport CSD's privacy assessment to ensure that **student data** will be protected with the addition of the new technology. The Department has not come to the conclusion that the District has demonstrated the necessary framework is in place to protect the privacy of data subjects and properly secure the data. As such, it is the Department's continued recommendation that the District delay its use of facial recognition technology.

Coyle Aff. Ex. 12.

69. As of May 30, 2019, NYSED still interpreted the meaning of student data in Education Law § 2-d to include the biometric information gathered, analyzed, and retained by Lockport's face recognition system.

70. Lockport revised its policy in February 2019 and again in early July 2019. The July 2019 revised privacy policy, Policy 5685 was adopted by the Lockport Board of Education at its August 7, 2019 school board meeting (the "August 2019 privacy policy"). Coyle Aff. Exs. 14, 15.

71. In the August 2019 privacy policy, Lockport removed "suspended students" as an explicit category of individuals whose personally identifiable information would be included in the Hot List. Coyle Aff. Ex. 15.

72. The August 2019 policy retained Lockport's wide discretion to include students on the Hot List via the policy's broad language allowing it to include "any persons that have been notified that they may not be present on District property" and "anyone believed to pose a threat based on credible information presented to the District." Coyle Aff. Ex. 15.

73. The August 2019 policy also provided that the Board of Education would receive a weekly update "when a suspended student or staff member is added to the database," thus acknowledging that students could still be included in the system. Coyle Aff. Ex. 15.

74. Notwithstanding these changes, as of August 23, 2019, NYSED stated that "the Department continues to work with the District to ensure that its policies on data privacy and security and its programs that utilize student's personally identifiable information comply with state and federal laws and take into consideration concerns raised by stakeholders regarding the civil rights of students." Coyle Aff. Ex. 16.

75. As late as October 3, 2019, NYSED confirmed that it considered the biometric information gathered, analyzed, and retained by Lockport's face recognition system to implicate student data as defined by Education Law § 2-d. Coyle Aff. Ex. 18.

76. Responding to public comments received in connection with the promulgation of the Part 121 Regulations, NYSED stated publicly that the "Department is aware of the concerns raised about the use of technology that utilizes biometric data in schools and continues to research and review these issues." Coyle Aff. Ex. 18.

Lockport's "Privacy Assessment" Process

77. Upon information and belief, Lockport provided NYSED with its first privacy assessment by letter dated November 20, 2018. Coyle Ex. 5. In response to NYSED's directions, it supplemented that initial privacy assessment at least 3 times, on February 25, 2019, on July 11, 2019 and on September 20, 2019.[2] Coyle Aff. Exs. 8, 15, 17.

78. NYSED also met with Lockport and its representatives, including representatives of SN Tech including Tony Olivo, K.C. Flynn, and Chris Blasko; on June 6, 2019. Coyle Aff. Ex. 13. The agenda for that meeting indicates that NYSED received a presentation of the Lockport face recognition system by SN Tech and a tour and observation of the system installed and in real time use.

79. Lockport appears to have consulted a presentation titled "AEGIS Face Recognition Accuracy Summary" produced by SN Tech sometime in August 2019 and a report by SN Tech's auditors, Freed Maxick CPA, dated October 30, 2019 (the "Freed Maxick

[2] Lockport also provided additional supplemental information concerning its face recognition system by letter dated February 14, 2020, including another amended version of Policy 2020 5685. Coyle Aff. Ex. 19.

Report").[3] Schwarz Aff. ¶¶ 30-50. But these documents do not show that the system does not create or maintain student data. Schwarz Aff. ¶¶ 30-50.

80. SN Tech's presentation, by its terms, addressed only the accuracy of the AEGIS system algorithm. Schwarz Aff. ¶¶ 40-41. The Freed Maxick Report does not address at all whether or not "no student data will be created or maintained by the operation of the District's facial recognition system." The Freed Maxick Report considered only whether SN Tech accurately had transcribed accurately certain summaries in a July 2019 NIST report relating to the AEGIS system algorithm. Schwarz Aff. ¶¶ 43-49.

81. However, even this report indicates that SN Tech significantly understated, or misrepresented, in its August 27, 2019 presentation, the AEGIS algorithm's accuracy with respect to the "False Match Rate for Black Males" and the "False Match Rate for Black Females" as reported in the July 2019 NIST report. Schwarz Aff. ¶¶ 47-48.

82. NYSED, upon information and belief, left the conduct of the Lockport "privacy assessment" largely, if not completely, to Lockport. Notwithstanding NYSED's Chief Privacy Officer's exercise of her power to require a school district to "perform a privacy impact and security risk assessment" in order to "ensure that [student] personally identifiable information is protected, " NYSED appears to have gone no further than issuing this order to Lockport under Education Law § 2-d(2)(c), and 8 N.Y.C.R.R. 121.13(b). Schwarz Aff. ¶ ¶ 33, 42; Coyle Aff. Exs. 6-8, 15, 17.

[3] As more fully set forth in the Schwarz Aff. ¶¶ 30-50, documents provided to New York State Assembly Member Monica Wallace by Lockport School Superintendent Michelle Bradley that appear to constitute Lockport's "privacy assessment" were recently produced publicly in response to a FOIL request directed to Lockport by the Lockport Union Sun & Journal. Lockport's submission to Wallace was a defense of the Lockport face recognition system in support of Lockport's request for an exemption from Wallace's proposed legislation banning face recognition systems from use in New York State schools.

83. NYSED was provided access to the underlying documentary materials generated by Lockport and its vendors in connection with the conduct of Lockport's privacy assessment, Coyle Aff. Exs. 8, 19. NYSED should have been aware that those documents did not support Lockport's assertion that its face recognition system did not "create or maintain any student data" as that term is defined in Education Law § 2-d.

NYSED's Abrupt Change of Position that Lockport's Face Recognition System Does Not Implicate Student Data

84. By letter dated September 20, 2019, Lockport advised NYSED that the District had come to the decision that no student data would be created or maintained by the operation of the District's face recognition system and that this position was reflected in the August 2019 draft privacy policy. Coyle Aff. Ex. 17.

85. NYSED responded to Lockport in its November 27, 2019 Determination. Coyle Aff. Ex.1. In accepting Lockport's representation that the Lockport face recognition system does not implicate the creation or maintenance of "student data," NYSED stated in the Determination that "this change reflects the progress we have made in discussions over many months [and] with additional revisions [to Lockport's August 2019 privacy policy], the Department believes that the Education Law § 2-d issues it has raised to date relating to the impact on the privacy of students and student data appear to be addressed." Coyle Aff. Ex.1.

86. NYSED had no new evidence at that time and none of the underlying facts concerning Lockport's face recognition system had changed.

87. NYSED appears to have focused solely on Lockport's representations that students are not in Lockport's reference database and thus not on the Hot List.

88. NYSED disregarded the Lockport face recognition system's other collection of student data.

89. The record before NYSED made clear that false positives—matches between students and people on the Hot List—are likely to occur with some frequency and Lockport has acknowledged that false matches are likely to occur. Coyle Aff. Exs. 2, 10, 19; Schwarz Aff. Ex. 12.

90. At all relevant times, NYSED was aware that most of the facial-recognition algorithms currently in use, including the algorithms used in SN Tech's AEGIS face recognition system, exhibit significant biases, with a high likelihood of misidentifying Asian American and African American people, as well as women and children. Schwarz Affidavit, ¶¶ 23-26. One-half of the students in Lockport schools are female and more than 25% of the students are students of color. Schwartz Aff. ¶¶ 28-29.

91. NYSED's decision ignored the record before it.

92. Just two months after NYSED's Determination, Michelle T. Bradley, Lockport's School Superintendent, confirmed, notwithstanding Lockport's prior representation to NYSED, that the Lockport face recognition system does, in fact, create and maintain student data. In her letter dated January 29, 2020 to New York State Assembly Member Monica P. Wallace, Superintendent Bradley stated that the AEGIS system does retain biometric or other data "where (a) the system issues an alert due to the matching of an image captured by a District camera with the photo of an individual placed in the AEGIS database consistent with the categories set forth above . . . ." In other words, at the very least, the system retains biometric data whenever there is an alert of a match within the system. Schwarz Aff. ¶ 39, Ex. 12.

93. Lockport's counsel likewise confirmed just two months after NYSED's Determination, that the system did create and maintain student data in its February 14, 2020

letter to NYSED. Coyle Aff. Ex. 19. Upon information and belief, NYSED has taken no action to reverse its November 27, 2019 Determination.

NYSED's Failure to Correct Lockport's Refusal to Comply with NYSED's November 27, 2019 Mandate to Revise Privacy Policy 2020-5685

94. Lockport failed to incorporate all of the changes to the privacy policy that NYSED otherwise required in the Determination.

95. NYSED permitted the Lockport face recognition system to be activated without ensuring that Lockport's Privacy Policy 2020 5686 contained the student privacy and protective provisions NYSED had mandated Lockport adopt.

96. In the Determination, NYSED proposed three additional changes to the Privacy Policy– the addition of a "scope" section, the addition of language to the "Maintenance of Databases" section, and removal of certain language on the 4th page of the policy or sufficient clarification that the language in that section does not apply to students. Coyle Aff. Ex. 2.

97. The Determination also required Lockport to communicate these changes to staff, parents, guardians, and students. NYSED directed Lockport to make these revisions in a minimal attempt to ensure the protection of Lockport students' PII in accord with Education Law § 2-d. Coyle Aff. Ex. 2.

98. Lockport disregarded NYSED's directions and failed to make all of NYSED's required revisions to the draft privacy policy.

99. Lockport activated its face recognition system on January 2, 2020 and the Lockport School Board approved the unchanged final version of the privacy policy on or about January 8, 2020. Coyle Aff. Exs. 2, 19.

100. NYSED failed to follow up with Lockport to ensure that Policy 2020 5685 reflects NYSED's revisions outlined in its November 27, 2019 letter.

NYSED's Determination Strips Lockport's Parents and Children of the Critical Protections of Education Law § 2-d

101. Over the course of NYSED's 18 months of engagement with the Lockport District, parents and students were not provided information about NYSED's ongoing involvement with Lockport on the operation of the system and the proposed privacy policies until Lockport Superintendent Bradley released a January 2, 2020 post on the Lockport schools website titled "January 2020 AEGIS Security System Update," available at https://www.smore.com/utzgy. Cheatham Aff. ¶ 5; Schwarz Ex. 4.

102. Lockport never hosted a town hall or any sort of meeting for students and families to learn more about the face recognition system. Cheatham Aff. ¶ 6.

103. Lockport has never released any information publicly about what data is generated by the face recognition system and how the data from the face recognition system would be used or who has access to it. Cheatham Aff. ¶ 7.

104. NYSED's Determination creates the paradoxical result that students and parents have none of the privacy protections that NYSED initially required Lockport to incorporate into its privacy policy. Shultz Aff. ¶¶ 7-8; Cheatham Aff. ¶¶ 12-13.

105. The Determination means that student biometric records can be shared with anyone and even sold for commercial purposes. If these records are shared with a third-party, the third-party can share it with even more people because redisclosure prohibitions contained in Education Law § 2-d simply do not apply. And, if someone hacks into the system, Lockport is not obligated to inform parents of the breach. Shultz Aff. ¶¶ 7-8; Cheatham Aff. ¶ 12.

106. Lockport's Policy 2020 5685 contains no language committing the District to not share or sell any of the student biometric information for the 60 days Lockport acknowledges

that student data is retained, leaving those student records entirely without protection. Coyle Aff. Ex. 2.

107. Pursuant to Respondents' Determination, the District does not need to manage all of its contractual relationships with third party vendors, such as SN Tech or Ferguson ECC, to ensure compliance with Education Law § 2-d. N.Y. Educ. Law § 2-d(3)(a), (c); 8 N.Y.C.R.R. § 121.2(c), § 121.3(b), § 121.3(c), § 121.6, § 121.9.

108. Thus, for example, SN Tech can use all of the student biometric data continuously being generated by the Lockport face recognition system to train the algorithms operating in the Lockport face recognition system for its own commercial benefit or for the commercial benefit of other facial recognition vendors.

109. Neither SN Tech nor Ferguson ECC, nor any other third party contractor with Lockport relating to the Lockport face recognition system, is obligated to submit a data security and privacy plan for each contract with Lockport to demonstrate how they will protect any information, including the surveillance camera data streams in the Lockport face recognition system. N.Y. Educ. Law § 2-d(5)(b)(3); 8 N.Y.C.R.R. § 121.6.

110. Lockport's Data Protection Officer does not have to oversee the data security and privacy of the Lockport face recognition system. 8 N.Y.C.R.R. § 121.8.

111. Respondents' Determination denies Lockport parents and students the right to file complaints about possible breaches or unauthorized releases of any information contained in the Lockport face recognition system, including the surveillance footage that is continuously queried against the AEGIS Hot List or reference database. N.Y Educ. Law § 2-d(7)(a); 8 N.Y.C.R.R. § 121.4.

112. Closed circuit surveillance camera systems are susceptible to remote compromise, due to inherent vulnerabilities in the systems and to the tendency of installation companies to configure them insecurely. Schwarz Aff. ¶ 18 n. 5.

113. Lockport parents and students will have no recourse if access to the Lockport face recognition system database which contains students' biometric information is breached, or if the camera system is breached or released in any unauthorized fashion.

114. Respondents' Determination means that the District has no obligation to be notified of, much less report, breaches of the Lockport face recognition system to NYSED, and no obligation to notify affected parents and/or eligible students of such breaches. N.Y Educ. Law § 2-d(6); 8 N.Y.C.R.R. § 121.6, § 121.10.

115. Lockport does not have to publish in its "parents bill of rights for data privacy and security" the "supplemental information" for each contract Lockport has entered into relating to the District's face recognition system as to how the third party contractors "will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements" of Education Law § 2-d and the Part 121 Regulations.

116. Lockport's 2020-5685 Policy does not adopt the NIST Cybersecurity framework as the standard for the Lockport face recognition system. Coyle Aff. Ex. 2. Lockport parents do not have the right to demand that the District, or its third party contractors, abide by the NIST Cybersecurity Framework as the standard for data privacy and security with respect to the Lockport face recognition system. N.Y Educ. Law § 2-d(3)(b)(3), § 2-d (5); 8 N.Y.C.R.R. § 121.5.

117. As a result of the Determination, Lockport's Data Protection Officer not have to oversee the data security and privacy of the Lockport face recognition system as Lockport's 2020-5685 Policy provides. 8 N.Y.C.R.R. § 121.8.

118. As a result of the Determination, NYSED's Chief Privacy Officer has no authority to impose any penalties on any of the Lockport face recognition system vendors and/or contractors for any breaches, or violations of Education Law § 2-d that may occur. N.Y. Educ. Law § 2-d(6)(d) and (e), § 2-d(7); 8 N.Y.C.R.R. § 121.11.

119. As a result of the Determination, NYSED's Chief Privacy Officer cannot exercise any of her oversight responsibilities with respect to the Lockport face recognition system. These oversight responsibilities include requiring Lockport to "act to ensure that personally identifiable information is protected in accordance with state and federal law and regulations, including but not limited to requiring an educational agency to perform a privacy impact and security risk assessment." *Id.;* 8 N.Y.C.R.R. §121.13.

NO PRIOR APPLICATIONS

120. No prior application for this or any similar relief has been made in any court.

STANDING

121. As parents of students in the Lockport City School District, Petitioners have suffered injury-in-fact as a result of the Determination. The denial of Education Law § 2-d rights, as enumerated in the law and in the Part 121 Regulations, and which are intended to protect Lockport students' biometric data, is significant. Because NYSED has made a determination that student data is not implicated by the Lockport face surveillance system, NYSED has stripped away a number of rights afforded under Education Law § 2-d and the Part 121 Regulations to Petitioners. Those rights include, but are not limited to, the rights that the

District and its third party face recognition technology vendors, such as Ferguson ECC and/or SN Tech, cannot not use any of the student PII generated by the Lockport face recognition system for commercial purposes and that the District and the third-party vendors would be required to notify parents in the event of any data breach or leak of student PII. Petitioners' interests and rights under Education Law § 2-d and the Part 121 Regulations have been violated by the Determination. Thus Petitioners have standing to sue to annul the Determination.

TIMELY FILING OF THIS ARTICLE 78 PROCEEDING

122. This case is timely filed, in accordance with New York State Governor's Executives Orders 202.8, 202.14, 202.28 and 202.38. This case has been filed electronically in accordance with Administrative Order of the Chief Administrative Judge of the Courts 115/2020.

CAUSE OF ACTION
Article 78 Relief

123. Petitioners repeat and reallege, as if set forth fully herein, the allegations contained in paragraphs 1-122.

124. Respondents' determination that the Lockport face recognition technology system does not implicate student data or its creation or maintenance is arbitrary and capricious and represents an abuse of discretion.

125. Therefore, the Court should rule in favor of Petitioners, annul, vacate and set aside the Determination, order Respondents to revoke NYSED's November 27, 2019 letter that gave Lockport permission to activate its face recognition system, and order Respondents to direct Lockport to de-activate its face recognition system.

PRAYER FOR RELIEF

WHEREFORE, Petitioners pray for judgment:

1. Annulling, vacating and setting aside the Determination made by the Respondents that no student data, as that term is defined in New York State Education Law § 2-d and its implementing regulations, 8 N.Y.C.R.R. Part 121, is implicated by the utilization of a face recognition technology system by the Lockport City School District and to declare that NYSED's Determination was affected by an error of law and that Respondents acted in an arbitrary and capricious manner, and/or abused their discretion in making it;

2. Ordering Respondents to revoke NYSED's November 27, 2019 letter that gave Lockport permission to activate its face recognition system and to direct Lockport to de-activate its face recognition system; and

3. Granting Petitioner all other relief as this Court deems just and proper.

Respectfully Submitted,

Dated: June 22, 2020
New York, New York

Beth Haroules (bharoules@nyclu.org)
Stefanie Coyle (scoyle@nyclu.org)
Molly Biklen (mbiklen@nyclu.org)
Lourdes Rosado (lrosado@nyclu.org)

NEW YORK CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 19th floor
New York, New York 10004
Telephone: 212-607-3300
Facsimile: 212-607-3318

Attorneys for Petitioners James Schultz and Renee Cheatham

VERIFICATION

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

JAMES SHULTZ, being duly sworn, states that he has read the foregoing Petition and knows the contents thereof; that the same is true to his own knowledge, except as to matters therein that are stated upon information and belief; and as to those matters, he believes them to be true.

JAMES SHULTZ

Sworn to and subscribed before me
this 22nd day of June, 2020

Notary Public

BETH HAROULES
Notary Public, State of New York
No. 02HA4890292
Qualified in New York County
Commission Expires March 30, 2023

VERIFICATION

STATE OF NEW YORK)
) ss:
COUNTY OF NEW YORK)

RENEE CHEATHAM, being duly sworn, states that she has read the foregoing Petition and knows the contents thereof; that the same is true to her own knowledge, except as to matters therein that are stated upon information and belief; and as to those matters, she believes them to be true.

RENEE CHEATHAM

Sworn to and subscribed before me
this 22nd day of June, 2020

Notary Public

BETH HAROULES
Notary Public, State of New York
No. 02HA4890292
Qualified in New York County
Commission Expires March 30, 2023