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. ____________ **AFFIDAVIT OF DANIEL SCHWARZ**

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

DANIEL SCHWARZ, being sworn, says:

1. I am a Privacy and Technology Strategist in the Policy Department of the New York Civil Liberties Union ("NYCLU"). I hold a BSc in computer science and media from the Hochschule der Medien, Stuttgart, Germany. I hold an M.F.A. from the University of California, Los Angeles. One of my principal areas of focus at the NYCLU is biometric recognition technology—in particular facial recognition. Except where otherwise noted, I have personal knowledge of the facts contained herein.

2. The NYCLU, the New York State affiliate of the American Civil Liberties

Union, has long advocated against the use of biometric surveillance in schools and other settings. The NYCLU first learned in the spring of 2018 that the Lockport School District ("Lockport" or the "District") was one of the first public school districts in the country to procure and utilize face recognition software technology in its K-12 schools.

3. The NYCLU began to engage in both public education and advocacy communications with NYSED from the point the NYCLU first became aware of Lockport's acquisition of a face recognition system in spring 2018, requesting that NYSED impose a moratorium on the utilization of face recognition technology in schools, for a variety of reasons, including that such capture of student biometric information violated Education Law §2-d.

4. Part of that effort included directing a FOIL request to Lockport concerning its face recognition system. I also conducted independent research on publicly available information relating to (i) Lockport's application for and receipt of New York State Smart School Bond Act funds to acquire its face recognition system; (ii) Lockport's known vendors for the face recognition system - SN Technologies Corp. based in Gananoque, Ontario, Canada ("SN Tech"), Ferguson Electric Construction Company ("Ferguson ECC"), and Corporate Screening and Investigative Group, LLC ("CSI Group"); and (iii) a variety of materials produced by the National Institute of Standards and Technology ("NIST").

5. Lockport, and its face recognition system vendors, SN Tech and Ferguson ECC, have no special expertise necessary to the conduct of a privacy impact and security risk assessment to ensure that student biometric information is protected. It is clear to me that at all times relevant to the issues at hand, that Lockport has operated under a naïve at best, if not cavalier, perspective on cybersecurity and student data privacy issues.[1]

[1] 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

6. Further, SN Tech, prior to its relationship with Lockport, had provided face recognition software systems predominantly to casinos, settings that were trying to guard against known criminal elements exploiting their casinos. SN Tech had no experience whatsoever working with schools much less student data that is protected by Education Law §2-d. Ferguson ECC has also admitted publicly it had no experience whatsoever with face recognition systems and was completely dependent on the manufacturer's representations concerning privacy and security issues.[2] Ferguson ECC, likewise, as electrical engineering contractor, clearly has no had no experience whatsoever handling student data that is protected by Education Law §2-d.

Lockport's Response to NYCLU's June 2018 FOIL Request

7. In June 2018, the NYCLU directed a FOIL request to Lockport seeking 22 categories of documents, including: records documenting Lockport's data access policies; policies governing the use of the facial recognition system; cybersecurity measures; and research and studies regarding the efficacy of facial recognition that was considered by the District. A

unrelated third party. After NYSED its expressed concerns about third-party vendors having access to private student and staff information, Lockport cancelled that third party contract, expressing what appeared to be bemused concern. 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." *See* Lockport Union Sun & Journal, Lockport school district cancels security contract, Connor Hoffman, April 11, 2019, https://www.lockportjournal.com/news/local_news/lockport-school-district-cancels-security-contract/article_b5612839-211e-53ff-a70b-c1de1f66abd6.html. A copy of this article is at Exhibit 1.

Lockport has already permitted SN Tech uncontrolled remote access to its 300 surveillance cameras as part of its testing arrangements – without notice to, or the consent of, Lockport's families or students. *See, e.g. Lockport School District to begin testing facial recognition system next week,* Connor Hoffman, Niagara Gazette, May 29, 2018, available at https://www.niagara-gazette.com/news/local_news/lockport-school-district-to-begin-testing-facial-recognition-system-next/article_817ec8d0-8221-11e9-a2fa-7307e9c8b65f.html. A copy of this article is at Exhibit 2.

[2] While Lockport contracted with Ferguson ECC to install the cameras that run the Aegis software, a Ferguson ECC principal indicated that "I don't have a lot of experience with the facial recognition technology, so we're relying on the manufacturer's engineers to set our expectations." *See* Thomas J. Prahaska, *Lockport schools turn to state-of-the-art technology to beef up security* (Buffalo News, May 20, 2108), https://buffalonews.com/2018/05/20/lockport-schools-turn-to-state-of-the-art-technology-to-beef-up-security/. A copy of this article is at Exhibit 3.

copy of the NYCLU's FOIL request to Lockport is attached at Exhibit 20 to the accompanying Affirmation of Stefanie D. Coyle, dated June 22, 2020 ("Coyle Aff.").

8. I reviewed the documents produced by Lockport in response to the NYCLU's FOIL request. Lockport certified, pursuant to Public Officer Law § 89(3)(a), the correctness of the copies of the responsive documents produced to the NYCLU. Lockport also certified that, with respect to a variety of records sought by the NYCLU, it either did not have possession of such responsive records or that such responsive records could not be found after diligent search had been conducted.

9. Lockport produced few, if any responsive documents relating to its decision to implement the face recognition system, documenting Lockport's data access policies; policies governing the use of the facial recognition system; cybersecurity measures; and research and studies regarding the efficacy of facial recognition that was considered by the District. Among the documents we did not receive are:

- Any policy that limits who will have access to the data collected by the facial recognition software, or any documentation explaining whether or not law enforcement agencies will have access.
- Any specific information about how the list of "unwanted persons" that will trigger an alarm when the cameras identify a possible intruder will be created or updated.
- There was also no confirmation of which law enforcement databases would be used to compile the "unwanted persons" list.
- Any procedures or training materials for staff to explain what will happen when an "unwanted person" is identified by the system or what will happen when the system makes a false identification.
- Any research or studies on the effectiveness of facial recognition technology consulted by the school board while developing this proposed use of millions of dollars of state funds.
- Any records reflecting research, studies, or data regarding the efficacy of facial recognition technology that was considered by the school.

10. The Lockport face recognition software is called "AEGIS." The AEGIS

software technology is trademarked and marketed by SN Tech. Lockport did not produce a contract with SN Tech or any materials relating to the AEGIS software system Lockport acquired for its face recognition system.

11. In March 2018, Lockport's School Board had awarded a bid to Ferguson ECC, an electrical engineering company, to install 300 enhanced surveillance cameras as well as software and other hardware components as part of its face recognition system. Lockport did not produce a contract with Ferguson ECC or any materials relating to the AEGIS software system Lockport acquired for its face recognition system, or any of the other hardware components installed by Ferguson ECC as part of the face recognition system.[3]

12. It has become apparent that Lockport does not hold the contract for the AEGIS software directly with SN Tech. 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.

13. The District did not produce any executed contracts or invoices directly between it and the vendor, SN Tech, or CSI Group, the firm that employs Lockport's security consultant.[4] Instead, the District produced only an invoice from Ferguson ECC that included a line item for $1,405,770 for "CSI/SN Tech Software Material" and $62,230 for "CSI/SN Tech Labor." *See* Coyle Aff. Ex. 24 n. 8.

14. Based on the documents produced, Lockport has no control over the AEGIS

[3] Deborah Coder, Lockport's Assistant Superintendent for Finance and Management, has been quoted indicating that "SN Technologies doesn't have a contract with Lockport. SN [Tech] is in effect a subcontractor with Ferguson [ECC]." *See* Ex. 3.

[4] J.A. "Tony" Olivo, the Lockport District security consultant for this project, has been paid as a "partner" of SN Technologies Corp.

software system and has no ability to modify, direct, or enforce the terms and conditions of the AEGIS software technology contract, which would be critical to ensuring that the operation of the face recognition system that Lockport has acquired is compliant with Education Law § 2-d.

Lockport's Face Recognition System

15. On January 2, 2020, Lockport activated AEGIS, the biometric face recognition technology system in all of its schools, from elementary to high school. AEGIS scans each person's face—including students—every time they walk by one of the numerous cameras throughout the schools and takes biometric measurements of each student's face.

16. The Lockport face recognition system engages in real-time analysis of biometric information from children, a process that will happen every second that this system is operating in a school.

17. Face recognition technology is a way of recognizing, and identifying, a human face through the automated, computational analysis of their facial features. Face recognition software, as used in the case of the 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 which constitutes a successful match depends on each system, implementation, and policy decision. Lockport has not released any of this information. The system's database of stored biometric samples of unwelcome people is controlled and populated by the Lockport School District.

18. Lockport has indicated publicly that it has installed 300 new closed circuit cameras 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. *See* Coyle Aff. Ex. 2; *see also Lockport City School District January 2020 AEGIS Security System Update,* available at https://www.smore.com/utzgy. A copy of this document is attached at Exhibit 4.

19. The quality of the images generated for automated analysis by a closed circuit camera system is highly dependent on correct installation of the cameras, positioning and view angle, lens characteristics, ambient lighting conditions, variable levels of crowding within the scope of the camera, and, ultimately, the direct camera-facing facial position of the intended targets of that automated analysis.[5]

20. The surveillance cameras are constantly recording all the faces of all the students that pass through or gather in the areas under camera surveillance. All of the student facial images that are recorded by the surveillance cameras are continuously analyzed and compared to the "persons of interest" database, or "Hot List," made by Lockport school administrators.

21. The "persons of interest" currently populating the Lockport reference database 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." *See* Coyle Aff. Ex. 2.

22. 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

[5] It is also important to note that 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.

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. All surveillance camera footage is retained for a period of 60 days, if not longer at the District's discretion. Privacy Policy 2020 5685 provides multiple exceptions allowing such data to be stored for longer periods of time.

23. As but one example, student biometric data is implicated whenever there is a misidentification that falsely matches a student to an individual in the database. Lockport's own privacy policy, 2020 5685, makes clear that misidentifications may occur and that certain data will be maintained in such instances.

Accuracy of Face Recognition Technology

24. Founded in 1901, the National Institute of Standards and Technology, or NIST, is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. *See* NIST General Information, available at https://www.nist.gov/director/pao/nist-general-information. A copy of this document is at Exhibit 5. NYSED established NIST's Cybersecurity Framework as the standard for educational agencies data security and privacy programs under N.Y. Education Law § 2-d. *See* 8 N.Y.C.R.R. § 121.5.

25. NIST, most importantly in this context, has issued a series of face recognition vendor tests (FRVT) to evaluate and assess different algorithms over the past twenty years. In a recent series of reports, NIST has evaluated the performance of one-to-one face recognition algorithms used for verification of asserted identities, and performance of one-to-many face recognition algorithms, such as the one used in the Lockport face recognition system, used for

identification of individuals in photo databases.[6] A recent report extended NIST's evaluations to document face algorithms accuracy variations disaggregated across demographic groups. This report, *NISTIR 8280 Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects,* was issued on December 12, 2019 and is available at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. A copy of this document is at Exhibit 6.

26. NIST's December 2019 report details the "empirical evidence" NIST found demonstrating that most of the face recognition algorithms in use currently exhibit "demographic differentials" that can diminish their accuracy based on a person's age, gender or race. The report examines 189 facial recognition algorithms by 99 vendors and shows significant biases, with a high likelihood of misidentifying Asian American and African American people, as well as women, children, and older people.[7]

27. NIST's December 2019 report reflects what many respected research academics have reported for the past several years relating to these demographic biases. *See, e.g.* Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, 1 IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE 32–41 (2019); Joy Buolamwini

[6] NIST has identified a significant "hardware" limitation with respect to the performance of face recognition algorithms. NIST indicates that while a reference database is generally comprised of "higher quality" or "clean" photos taken at a good angle, those reference database images are compared with surveillance footage that provides images at bad angles (usually overhead or at distance) in an uncontrolled lighting situation. More often than not, these circumstances will also cause "false positive" identifications, i.e. the erroneous association of samples of two persons which occur when the algorithm determines that the digitized faces of two people are similar. These environmental circumstances occur no matter how high resolution the surveillance cameras are.

[7] Asian and African American people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search. Native Americans had the highest false-positive rate of all ethnicities, according to the study, which found that systems varied widely in their accuracy. The faces of African American women were falsely identified more often in the kinds of searches used by police investigators where an image is compared to thousands or millions of others in hopes of identifying a suspect. Women were more likely to be falsely identified than men, and the elderly and children were more likely to be misidentified than those in other age groups, the study found. Middle-aged white men generally benefited from the highest accuracy rates.

& Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), available at http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Copies of these studies are at Exhibits 7 and 8, respectively.[8]

28. The stakes with respect to misidentifications that might occur as a result of the operation of the Lockport face recognition system are particularly high in Lockport where half of the students in Lockport schools are female and more than 25% of the students are students of color.[9]

29. NYSED's own data demonstrates the existing disproportionality in disciplinary sanctions received by students of color in the Lockport District. During the 2015-2016 school year in the District, black students made up just 12.3% of the student population, but represented more than a quarter of the students receiving out of school suspensions. The data also indicated that students of two or more races represented 5.9% of the student population in Lockport, but 15% of the students receiving out of school suspensions.[10]

Materials Provided by NYSED in Response to NYCLU's FOIL Request

[8] IBM, joined by Amazon and Microsoft, in fact, have all announced that they will halt the sale of facial recognition technology to police because the technology has been shown to suffer from bias along lines of age, race, and ethnicity, which can make the tools unreliable for law enforcement and security and ripe for potential civil rights abuses. *See Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*, Jay Greene, Washington Post June 11, 2020 12:30 p.m. available at https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/. A copy of this article is at Exhibit 9.

In addition, the New York State Smart School Bond Act Review Board will no longer approve applications seeking Smart Schools Bond Act funding to acquire and install facial recognition technology or other similar self-learning analytic software. This announcement is on their website landing page http://www.p12.nysed.gov/mgtserv/smart_schools/.

[9] Lockport City School District at a Glance, 2017-2018, https://data.nysed.gov/profile.php?instid=800000041703. A copy of this data is at Exhibit 10.

[10] Due to a suspension of federal regulations that mandate State reporting of disproportionality data, 2015-2016 is the latest year for which this data is available. 2015-2016 Civil Rights Data Collection data, https://ocrdata.ed.gov/Page?t=d&eid=31160&syk=8&pid=2539&Report=6. A copy of this data is at Exhibit 11.

30. The NYCLU sent a FOIL request to NYSED dated January 2, 2020 ("NYCLU's January 2020 FOIL Request") to learn more about NYSED's decision to approve Lockport's face recognition system. *See* Coyle Aff. Ex. 28.

31. The NYCLU's January 2020 FOIL Request sought seven categories of records regarding Lockport's face recognition system, including, among other things, records reflecting NYSED's communications with Lockport, including the September 20, 2019 letter described in NYSED's November 27, 2019 Determination, records reflecting any "privacy assessment" undertaken by NYSED with regard to Lockport's facial recognition system; records reflecting accuracy tests and evaluations of Lockport's facial recognition technology and, if existing, on representative datasets, disaggregated by age, gender, and race; records reflecting accuracy evaluations of the shape-based recognition system and descriptions of what testing data was used; and records reflecting research, studies, experts, vendors, or data regarding the efficacy of facial recognition technology that was consulted or considered by NYSED in its evaluation of Lockport's face recognition system.

32. NYSED produced 16 documents responsive to the NYCLU's January 2020 FOIL Request on May 14, 2020.[11]

33. I have reviewed the documents NYSED produced in response to the NYCLU's January 2020 FOIL. If these are the only documents responsive to the NYCLU's FOIL, it is clear that NYSED left the conduct of the Lockport "privacy assessment" largely, if not completely, to Lockport and its vendors. NYSED appears to have conducted no independent analysis of the Lockport face recognition system and merely accepted, without question or analysis, any of the information provided it by Lockport and its vendors.

[11] A number of those documents are attached as exhibits to the Coyle Aff.

Lockport “Privacy Assessment” Materials Provided in Response to FOIL Request by Lockport Union Sun & Journal

34. The Lockport Union-Sun & Journal sent a FOIL request to Lockport dated February 7, 2020 requesting production of any communications between Lockport and New York State Assembly Member Monica Wallace between January 1, 2019 and February 7, 2020.

35. Lockport produced 28 pages of responsive documents to the Lockport Union Sun & Journal on March 6, 2020. The documents include the Lockport cover letter transmitting the documents as well as a four page letter dated January 29, 2020 between Lockport’s Superintendent of Schools, Michelle T. Bradley and Assembly Member Wallace, a copy of Lockport Privacy Policy 2020-5685, and an “Independent Accountant’s Report” dated October 30, 2019 that was prepared by Freed Maxick CPA (the “Freed Maxick Report”). The Freed Maxick Report includes selected excerpts from a July 31, 2019 NIST report. The documents produced by Lockport in response to the Lockport Union Sun & Journal are available at https://www.scribd.com/document/450912575/DOC030620-03062020152848. A copy of these documents are attached as Exhibit 12.

36. Superintendent Bradley’s cover letter to Assembly Member Wallace, and the supporting documents, appears to provide an outline of the “privacy assessment” conducted by Lockport that resulted in Lockport’s conclusion communicated to NYSED in fall 2019 that the Lockport face recognition system does not “create or maintain any student data.”

Lockport’s Representations about Student Biometric Data Retained by its Face Recognition System

37. I have reviewed both NYSED’s FOIL production to the NYCLU and Lockport’s FOIL documents obtained published by the Lockport Union Sun & Journal.

38. NYSED's November 27, 2019 Determination[12] that Lockport's face recognition system did not "create or maintain any student data" appears to have rested on Lockport's representations in the fall of 2019 that the face recognition did not "create or maintain any student data." Notwithstanding Lockport's apparent representations to NYSED in the fall of 2019 in this regard, Lockport offered a different representation to Assembly Member Wallace about what student biometric information was "retained" by the face recognition system just two months after NYSED's Determination was issued.

39. Superintendent Bradley stated to Assembly Member Wallace in her letter dated January 29, 2020 that the AEGIS system "does not retain any biometric or other data during its operation **except** under circumstances 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 […]" (emphasis supplied). *See* Ex.12.[13]

Documents that Lockport Obtained During the Course of Lockport's Conducting the "Privacy Assessment" Mandated by NYSED

40. Lockport provided NYSED with information provided to it by SN Tech relating to the algorithm utilized in the District's face recognition system on or about February 25, 2019. *See* Coyle Aff. Ex. 8. Lockport advised NYSED that the materials from SN Tech's "facial recognition partner id3 Technologies" demonstrated the accuracy of the Lockport face recognition system (the "id3 Technology Overview"). Lockport's attorneys claimed "[b]ased on application of the facial recognition benchmark adopted by the National Institute of Standards and Technology ("NIST," the same entity incorporated into the proposed implementing

[12] *See* Coyle Aff. Ex. 1.

[13] Lockport made this same representation to NYSED by letter dated February 14, 2020. See Coyle Aff. Ex. 19.

regulations for Education Law § 2-d), testing of the Aegis System facial recognition software demonstrated that the software has "excellent accuracy."

41. I have reviewed the id3 Technology Overview produced by NYSED in response to the NYCLU's January 2020 FOIL Request. *See* Coyle Aff. Ex. 8. The document does not confirm the accuracy of the AEGIS system algorithm and, further, does not at all address whether or not "no student data will be created or maintained by the operation of the District's facial recognition system." The id3 Technology Overview document is a marketing document in which id3 Technologies notes that its face matching algorithm has "excellent tradeoff between accuracy, speed and template size." The document provided a graph showing "error tradeoff characteristics for white females, black females, black males and white males." That graph does not support Lockport's representations that its face recognition system is expected to be accurate 124 of every 125 alerts for white males, 99 of every 100 alerts for black males, and 49 of every 50 alerts for females (both white and black).

42. NYSED has produced no materials indicating it evaluated the representations made by Lockport in its February 2019 submission.

43. I have also reviewed the Freed Maxick Report.[14] It appears, in connection with Lockport's "privacy assessment" process, that representatives of SN Tech made a presentation to Lockport on or about August 27, 2019, titled "AEGIS Face Recognition Accuracy Summary." *See* Ex. 12.

44. According to the Freed Maxick Report, statements made by SN Tech at its

[14] Lockport provided NYSED with a copy of the Freed Maxick Report by letter dated February 14, 2020. *See* Coyle Aff. Ex. 19. Based on the materials produced in NYED's response to NYCLU's 2020 FOIL Request, NYSED did not evaluate any of these materials.

August 27, 2019 presentation purported to confirm the accuracy of SN Tech's AEGIS system algorithm. The Freed Maxick Report examined certain assertions made by SN Tech at the presentation and then itself purported to confirm the accuracy of SN Tech's AEGIS system algorithm. *See* Ex. 12.

45. The Freed Maxick Report does not confirm the accuracy of the AEGIS system algorithm and, further, does not at all address whether or not "no student data will be created or maintained by the operation of the District's facial recognition system." Freed Maxick, SN Tech's accountants, merely assessed whether SN Tech accurately transcribed "assertions made in [SN Tech's] August 27, 2019, presentation titled 'AEGIS Facial Recognition Accuracy Summary' […] which detailed the testing results of its face recognition technology as reported by the National Institute of Standards and Technology (NIST) within its 'Ongoing Face Recognition Vendor Test,' dated July 31, 2019 ('NIST Report')." *See* Ex. 12.

46. The Freed Maxick Report actually indicates that SN Tech significantly understated, or misrepresented, the AEGIS algorithm's accuracy with respect to the "False Match Rate for Black Males" and the "False Match Rate for Black Females" in its August 27, 2019 presentation. *See* Ex. 12.

47. According to Freed Maxick, SN Tech reported in its August 2019 presentation that "Black Males are 2 times more likely than White Males to have a False Match." The NIST Report, however, indicates that the False Match Rate for Black Males is 4 times more likely than White Males. SN Tech's misrepresentation understates the Black Male vs. White Male false match rate by 100%. *See* Ex. 12.

48. SN Tech also apparently represented that "Black Females are 10 times more

likely than White Males to have a False Match." The NIST Report, however, indicates that the False Match Rate for Black Females is 16 times more likely than White Males. SN Tech's misrepresentation understates the Black Female vs. White Male false match rate by 60%. *See* Ex. 12.

49. The accuracy of the AEGIS algorithm used in the Lockport face recognition system is not proven by the partial set of documents SN Tech apparently offered to Lockport, and Lockport shared with NYSED, as part of SN Tech's August 27, 2019 presentation titled "AEGIS Face Recognition Accuracy Summary."

50. If these documents are the totality of materials Lockport relied upon in conducted the "privacy assessment" mandated by NYSED, these documents provided no support for Lockport's conclusion that its face recognition technology system does not create or maintain student data.

DANIEL SCHWARZ

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