BY ELECTRONIC MAIL

Interim Commissioner Shannon Tahoe
New York State Education Department
89 Washington Avenue
Albany, NY 12234

January 2, 2020

Dear Interim Commissioner Tahoe:

We write concerning the New York State Education Department's ("NYSED" or the "Department") November 27, 2019 letter to the Lockport City School District ("Lockport" or the "District") regarding its proposed use of facial recognition technology in its schools.[1] NYSED's letter appears to give Lockport explicit permission to utilize its biometric surveillance system, despite unanswered questions about the system's functionality and the very real risks of this technology. In fact, Lockport clearly interpreted the letter as providing permission and has activated its cameras today, January 2.[2]

NYCLU
ACLU of New York

125 Broad St. 19th Fl.
New York NY 10004
(212) 607-3300

Donna Lieberman
Executive Director

Robin Willner
President

NYSED had been consistent in expressing its concerns with Lockport's facial recognition system over the last 18 months.[3] The Department seemed to believe that further study was required before facial recognition technology could be introduced into the public schools. Therefore, NYSED's most recent letter came as a surprise. We fear that the Department's decision was made without a complete and accurate set of facts and was based on a misunderstanding of how the system works. We conclude that allowing Lockport to utilize this biometric surveillance system in its schools, based on current information, is arbitrary and capricious.

We reach this conclusion for several reasons. First, the surveillance system will not advance the District's stated objectives. Second, contrary to Lockport's claim, the system will inevitably implicate student data. Third, the approval of this system is premature given current circumstances, and fourth, particularly given the known harms of facial recognition technology. Fifth, the District has not yet met the conditions imposed by NYSED's apparent approval. Finally, this approval process has been plagued with a lack of transparency and the public should have access to more information about the system.

We request that NYSED rescind its apparent approval to provide time for complete transparency about the system (including NYSED's independent analysis of the safety and propriety of the system), to receive meaningful and informed community input, and to complete the ongoing regulatory and legislative processes that will have serious implications for this technology. NYSED should not allow Lockport's students, teachers, and community members to be test subjects for inaccurate and invasive technology.

---

[1] Temitope Akinyemi, November 27, 2019 Letter to Michelle Bradley (the "November 27 Letter").
[2] *January 2020 AEGIS Security System Update*, https://www.smore.com/utzgy.
[3] Davey Alba, *The First Public Schools in the US Will Start Using Facial Recognition Next Week*, May 30, 2019, Buzzfeed News, https://www.buzzfeednews.com/article/daveyalba/lockport-schools-facial-recognition-pilot-aegis ("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.").

I. NYSED's Approval of Lockport's Technology is Arbitrary and Capricious[4]

a. Lockport's Technology Will Not Advance the District's Stated Objectives

Lockport's biometric surveillance system is not a solution for the problem it is purportedly trying to address. Lockport has repeatedly stated that it obtained its facial recognition system in order to prevent school shootings and specifically wanted to include suspended students in the search database of unwanted persons (the "Hot List") to guard against such shootings.[5] However, the District purchased a Raptor visitor management system which should be able to prevent certain types of unauthorized individuals from entering school premises,[6] including those listed in the current iteration of the privacy policy: staff who are suspended or on administrative leave, Level 2 or 3 sex offenders, anyone prohibited to enter District property by a court order, and anyone believed to "pose a threat based on credible information presented to the District."[7] The Raptor system could presumably also be utilized to prevent suspended students from entering school buildings, if school staff are unable to perform this function.

NYCLU
ACLU of New York

Since suspended students have been removed from the Hot List, neither the District nor NYSED has offered an explanation as to how the system will accomplish their goal of preventing school shootings or why the current tools that the District has are inadequate.

b. The System Will *Implicate Student Data and Should be Subject to Heightened Security Obligations*

In its November 27 Letter, NYSED appears to agree with Lockport[8] that the data generated from the facial recognition system will not be "student data" and that even if it is, that it will not be "created or maintained" by the system.[9] This is absurd. It reflects, at best, a fundamental misunderstanding of how this technology functions.

---

[4] *Ward v. City of Long Beach*, 20 N.Y.3d 1042, 1043 (N.Y. 2013) ("An action is arbitrary and capricious when it is taken without sound basis in reason or regard to the facts.") (*internal citations omitted*).

[5] Madison Carter, *I-Team: Lockport Schools pull faces from facial recognition system; will only track guns*, WKBW Buffalo, September 9, 2019, https://www.wkbw.com/news/i-team/i-team-lockport-schools-pull-faces-from-facial-recognition-system-will-only-track-guns ("We believed from the get-go that suspended students, based on studies from shootings in our country where much too often there have been - they've included students who are expelled or familiar with the schools. So we believed that category is something we should consider," said [Michelle] Bradley.).

[6] Fall 2019 Welcome Back Newsletter, Lockport City School District, https://www.lockportschools.org/welcomeback ("The Raptor Visitor Management System was implemented in January 2019 and requires all visitors to show a government issued photo upon arrival.").

[7] December 11, 2019 Operation and Use of Security Systems/ Privacy Protections, Policy 5685, https://www.lockportschools.org/cms/lib/NY19000563/Centricity/domain/1300/5000/5685.pdf.

[8] It appears that NYSED has accepted the District's nonsensical representations that the system will not "create or maintain" any "student data" without question. Conspicuously absent from the letter is any indication that NYSED has independently come to this conclusion.

[9] November 27 Letter, (The District "has come to the decision that no student data will be created or maintained by the operation of the District's facial recognition system, and that this position is now reflected in" its revised policy.). The phrase "create[] and maintain[]" appears in neither Education Law § 2-d nor its proposed implementing regulations. Should NYSED intend to use this standard going forward, it must engage in public rulemaking with respect to its proposed regulations. But, even if this newly-invented

Face surveillance works by comparing data points associated with an individual's facial characteristics to those associated with photos on the Hot List.[10] This comparison is usually conducted by an algorithm which analyzes facial geometry and features to determine whether there is a match with photos on the Hot List. In order for Lockport's system to determine whether there are any matches to the individuals on the Hot List, it has to analyze all faces that appear in the camera frames.[11] 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 facial recognition system, including students.[12] The data captured by the system, which clearly falls within the definition of "student data" in Education Law § 2-d, is analyzed by the system to determine whether a match has been identified, even if it is held only briefly. Regardless of whether there are student photos populating the Hot List, "student data" will necessarily be "maintained" by the system every time a student's face is analyzed and found to not be a match.[13]

NYCLU
ACLU of New York

NYSED appears to focus solely on the fact that students are not on the Hot List, rather than the real-time collection, analysis, and retention of biometric information from children, which will happen every second that this system is operating in a school. According to Lockport's own privacy policy, images from the system will be stored for up to 60 days, with multiple exceptions allowing such data to be stored for longer periods of time.[14] Student data will also be implicated whenever there is a misidentification that falsely matches a student to an individual in the database.[15]

NYSED's misconception has serious consequences. Its determination that the data implicated by the facial recognition system is not "student data" could allow the transmittal

---

standard were to be adopted by NYSED, the District cannot meet it, as the system would still "create and maintain" student biometric data, as stated above.

[10] "Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. Unlike many other biometric systems, facial recognition can be used for general surveillance in combination with public video cameras, and it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject." ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.

[11] Madison Carter, *I-Team: Lockport Schools pull faces from facial recognition system; will only track guns*, WKBW, September 9, 2019, (Dr. Rob LiPuma, Director of Technology, Data, Security and Communications stated "This system works with the CCTV cameras and as footage is being collected it's analyzing the footage being collected trying to find a match for something that's in the database.").

[12] *Id.* ("'[The] cameras actually are continuous video that's based on movement in hallways or at doorways,' said LiPuma. 'The cameras are recording whatever is going on in those areas.'").

[13] We hope and assume that the District's position (and NYSED's adoption of it) that the system will not create or maintain student data is not based on an overly narrow definition of the words "create" or "maintain."

[14] Operation and Use of Security Systems/ Privacy Protections, Policy 5685, https://www.lockportschools.org/cms/lib/NY19000563/Centricity/domain/1300/5000/5685.pdf. "The security cameras only capture images and no images collected from security systems are stored for longer than 60 days, unless the information is being evaluated or preserved as part of an investigation, or retained in conjunction with a log of confirmed security alerts."). The maintenance of this data also allows the District to retroactively utilize the software to track individuals.

[15] *Id.*

and use of sensitive student information without the security measures required by state and federal law to keep it safe.[16]

c. NYSED's Approval of Lockport's System is Premature

The timing of the decision to allow Lockport to go forward is premature and contributes to the appearance that NYSED's decision was made without sufficient facts and consideration. In June 2019 and then again in September 2019, NYSED explicitly prohibited Lockport from testing its facial recognition technology.[17] 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.[18]

NYCLU
ACLU of New York

Parallel to the review process in Lockport, NYSED has been engaged in a nearly year-long regulatory process to finalize and issue regulations under Education Law § 2-d. NYSED continued to collect comments on the most recent proposed regulations until the second week of December. It is premature for NYSED to approve the use of a biometric surveillance system while the regulations governing the protection of student data are not yet final.[19]

The timing of NYSED's pronouncement is even more troubling given that the Governor signed legislation this year that would create a commission on artificial intelligence, robotics, and automation to be convened in 2020. This commission is charged to study and address issues related to the use of artificial intelligence across the state and to consider regulation, including of biometric surveillance in schools.[20] The creation of this commission indicates that our state government believes this issue is worth serious and careful consideration by experts.

---

[16] N.Y. Educ. Law § 2-d; New York SHIELD Act, N.Y. Gen. Bus. Law § 899-aa (McKinney); Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232; 34 C.F.R. § 99 et seq.

[17] Connor Hoffman, *School district reminded not to test Aegis*, The Lockport Journal, September 5, 2019, https://www.lockportjournal.com/news/local_news/school-district-reminded-not-to-test-aegis/article_37223a25-cf41-5ef3-a934-b983e97425a6.html ("Department staff has contacted the district to reiterate our directive to cease the testing and utilization of facial recognition technology until further notice.")

[18] Elizabeth R. Berlin, Proposed Adoption of Part 121 to the Regulations of the Commissioner Relating to Student Data Privacy and Security, Comment 38, October 3, 2019, https://www.regents.nysed.gov/common/regents/files/1019p12hed1.pdf.

[19] The NYCLU has submitted multiple comments during the regulatory process urging NYSED to more carefully address the use of biometric surveillance in schools and to place a moratorium on its use. NYSED's response has been inadequate, stating: "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. No change is necessary." Elizabeth R. Berlin, *Proposed Adoption of Part 121 to the Regulations of the Commissioner Relating to Student Data Privacy and Security*, October 3, 2019, https://www.regents.nysed.gov/common/regents/files/1019p12hed1.pdf.

[20] *Governor Cuomo Signs Legislation Creating New State Commission to Study Artificial Intelligence and Robotics*, July 24, 2019, https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-creating-new-state-commission-study-artificial-intelligence; Lizbeth Beltran, *State creates commission to study the impact of robots*, Crain's New York, July 26, 2019, https://www.crainsnewyork.com/politics/state-creates-commission-study-impact-robots.

Moreover, there is pending state legislation[21] that would require a commission to specifically study the effects of biometric surveillance technology on children and put a moratorium on its use in schools until the study is completed. This bill passed quickly in the New York State Assembly with a bipartisan vote of 128 to 19.[22] It will be reintroduced during the legislative session that begins in January 2020 and it is highly likely that it will pass both houses. Given this pending legislation that would block Lockport and other districts from using biometric surveillance technology, it is rash for NYSED to approve this system at this juncture.

d. Moving Forward with this Technology Puts Kids at Risk

NYCLU
ACLU of New York

It is irrational for NYSED to approve the use of biometric surveillance when there are so many risks involved[23] – risks recognized by the private sector, cities across the United States[24], and countries throughout the world that have already banned the technology.

The ethics board of Axon, one of the largest manufacturers of police body-worn cameras, banned the use of facial recognition technology on its cameras earlier this year, stating, "[f]ace recognition technology is not currently reliable enough to ethically justify its use."[25] The Swedish Data Protection Authority issued its first fine under the General Data Protection Regulation after a high school experimented with a facial recognition system for taking attendance. The Authority found that although the data was collected consensually, it was still unlawful to gather the data because of "the clear imbalance between the data subject and the controller."[26]

---

[21] A 6787B (Wallace)/ S 5140A (Kavanagh), https://assembly.state.ny.us/leg/?default_fld=&bn=A06787&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y.

[22] *Id.* The bill also has widespread support. *See* Stop Student Surveillance Sign On Letter, June 18, 2019, https://www.nyclu.org/sites/default/files/biometric_sign_on_letter_final_6.18.19.pdf.

[23] This decision is also problematic due to the inevitability of the operation of the system leading to the potential violation of the Constitutional rights of students, parents, teachers, and other community members who pass through the school district. *See* U.S. Const. amends. I, IV, and XIV. Proceeding with this system may open up Lockport and other districts to liability, particularly as students must comply with New York's compulsory education statute and therefore are required to attend school and be subjected to this system.

[24] Kristin Lam, *Portland, the largest city in Oregon, plans to propose first facial recognition ban affecting private companies*, USA TODAY, December 3, 2019, https://www.usatoday.com/story/tech/2019/12/03/facial-recognition-portland-oregon-ban/2601966001/; Tom McKay, *Berkeley Becomes Fourth U.S. City to Ban Face Recognition in Unanimous Vote*, GIZMODO, October 16, 2019, https://gizmodo.com/berkeley-becomes-fourth-u-s-city-to-ban-face-recogniti-1839087651; City and County of San Francisco - File #: 190110, May 31, 2019, https://sfgov.legistar.com/LegislationDetail.aspx?ID=3850006&GUID=12FC5DF6-AAC9-4F4E-8553-8F0CD0EBD3F6; *Oakland bans city use of facial recognition software*, ENGADGET, July 17, 2019, https://www.engadget.com/2019/07/17/oakland-california-facial-recognition-ban/; *Somerville City Council moves to ban government face surveillance*, ACLU MASSACHUSETTS (2019), June 24, 2019, https://www.aclum.org/en/news/somerville-city-council-moves-ban-government-face-surveillance.

[25] Charlie Warzel, *A Major Police Body Cam Company Just Banned Facial Recognition*, The New York Times, June 27, 2019, https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html.

[26] Melanie Ehrenkranz, *Sweden's First GDPR Fine Goes to a High School Piloting Facial Recognition Attendance*, Gizmodo, August 27, 2019, https://gizmodo.com/swedens-first-gdpr-fine-goes-to-a-high-school-piloting-1837616893.

With each passing day, there is additional reporting about precisely how inaccurate this type of technology is, particularly when used to identify women, young people, and people of color.[27] Additionally, the use of facial recognition technology raises significant concerns about information-sharing with law enforcement agencies, including ICE. Finally, these systems are vulnerable to hacking, thus putting sensitive student information in jeopardy.[28]

With its decision to allow Lockport to go forward, NYSED has opened the floodgates to a new reality of high-tech student surveillance with potentially devastating consequences. Even as other governments adopt bans on this unethical and harmful technology, New York will spend our public dollars subjecting students to it.

NYCLU
ACLU of New York

e. Lockport Has Not Yet Met NYSED's Conditions for Approval of the System

Lockport's privacy policy does not and cannot address the litany of harms associated with biometric surveillance. Regardless of what additional changes may be made to the policy, facial recognition is an inaccurate and biased tool that will invade the privacy of students, staff, parents, and community members in schools.

However, in its November 27 Letter, NYSED proposed three additional changes to the 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. Finally, the Letter requires Lockport to communicate these changes to staff, parents, guardians, and students.

Despite these mandates, Lockport failed to incorporate these changes during the latest revision of the policy discussed at Lockport's December 11, 2019 school board

---

[27] Natasha Singer and Cade Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, The New York Times, December 20, 2019, https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html; Joseph Goldstein and Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*., The New York Times, August 1, 2019, *available at* https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html?action=click&module=Top%20Stories&pgtype=Homepage; Steve Lohr, *Facial Recognition Technology is Accurate, if You're a White Guy*, The New York Times, February 9, 2018, *available at* https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer; 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 & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[28] Justin Murphy, *School districts on guard against ransomware attacks after recent surge*, Rochester Democrat and Chronicle, July 30, 2019, *available at* https://www.democratandchronicle.com/restricted/?return=https%3A%2F%2Fwww.democratandchronicle.com%2Fstory%2Fnews%2Feducation%2F2019%2F07%2F30%2Fschool-districts-ransomware-attacks-syracuse-rochester-cybersecurity%2F1806440001%2F ("In some ways, small school districts are the most tempting target, as they likely have fewer safeguards in place.").

meeting.[29] Yet, this version of the policy is set to be approved at its January 8, 2020 meeting.[30] It is irrational for NYSED to allow Lockport to proceed with its system while the conditions-precedent to its approval have not yet been met.

II. NYSED's Approval Process Has Lacked Transparency and Many Unanswered Questions Remain

Over the past 18 months, the NYCLU has sent 10 letters and comments to NYSED regarding Lockport's biometric surveillance plans and student data privacy. We have received only two responses – one via letter in August 2018 and one via email in August 2019. In its August 2018 letter, NYSED stated that the agency was undertaking a "privacy assessment" with regard to Lockport's use of facial recognition technology. However, it is still unclear what this process entailed; what materials, if any, were reviewed; what vendors, if any, NYSED met; whether outside research and analysis on face surveillance and/or shape detection technology was conducted; whether and how the systems will be audited; and what criteria NYSED used to evaluate the system.

In addition to a lack of transparency in the approval process, there is also a lack of public information about the actual Lockport systems. Neither NYSED nor the District has provided any information regarding the capabilities and accuracy measurements of the facial recognition system. We still do not know whether the specific system the District intends to use has different accuracy rates for people of different races, ages, or genders. There is even less information about the District's object recognition system, the existence of which is only mentioned once in its privacy policy. We also continue to have questions and concerns about how this technology was procured and the public has yet to see the actual contract between the District and its vendor, as the District contracted directly with an electric company which then, apparently, may have a contractual relationship with the biometric surveillance vendor.[31]

The lack of public input and complete disregard for transparency from both the District as well as NYSED is concerning. We seek additional information in the attached

---

[29] The November 27 Letter required that Lockport "add the language used in your cover letter to the Maintenance of Databases section to reflect that 'no student data will be created or maintained by the operation of the District's facial recognition system'" but no such language was added to that section. The November 27 Letter also required that the district "remove the language on page 4 under 'Privacy' that states that '[i]n furtherance of that purpose, such information may be used as appropriate for disciplinary reasons, and may be shared with law enforcement or other governmental authorities as required or permitted by law' or clarify in the policy that this language does not apply to students." On page 4 of the current iteration of the Lockport policy, the only revision was the removal of the words "may be used as appropriate for disciplinary reasons." Nothing was added or removed to address the sharing of student data with law enforcement or other governmental authorities. See Policy 5685, "Operation and Use of Security Systems/Privacy Protections" https://www.lockportschools.org/site/handlers/filedownload.ashx?moduleinstanceid=10176&dataid=30849&FileName=Policy%205685%20Review%2012-11-19%20and%20Adoption%201-8-20.pdf.

[30] Lockport activated its system today, January 2, 2020, despite the fact that the amendments to its own privacy policy are not yet finalized.

[31] In its response to our June 2018 Freedom of Information Law request, the District produced an invoice from Ferguson Electric that included a line item for $1,405,770 for "CSI/SN Tech Software Material" and $62,230 for "CSI/SN Tech Labor." The District did not produce an executed contract directly between it and the vendor, SN Technologies/Corporate Screening and Investigative Group, LLC.

request made pursuant to the New York Freedom of Information Law ("FOIL")[32], attached as Exhibit A.

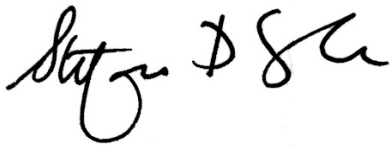
III. Conclusion

The harms of facial recognition technology and other biometric surveillance are well-studied and well-documented. NYSED has disregarded this information, neglecting its responsibility to safeguard student data and protect the students of New York by greenlighting a face surveillance system in Lockport's schools. It appears that the Department has taken an uncritical look at the deployment of this technology and has disregarded the precedential impact of its decision.

NYCLU
ACLU of New York

Given all of the concerns raised above and significant unanswered questions, NYSED should immediately rescind its decision to allow Lockport to proceed with the use of its facial recognition system. We ask that you inform us promptly of your response to this letter. I can be reached at 212-607-3315 or scoyle@nyclu.org.

Sincerely,



Stefanie D. Coyle
Deputy Director, Education Policy Center

cc: Tope Akinyemi, Chief Privacy Officer, NYSED
Members of the Board of Regents

[32] N.Y. PUB. OFF. LAW § 84, et seq.

Exhibit A

As you know, FOIL requires a response within five business days of your receipt of this letter. Please provide an estimated timeframe within which the requested records are to be produced. If for any reason any portion of this request is denied, please inform us of the reasons for the denial in writing and provide the name and address of the person or body to whom an appeal should be directed. If you determine that any portion of the requested records are exempt from disclosure pursuant to FOIL, please redact only the material claimed as exempt, inform us of the basis for the exemption claim, and furnish copies of those portions of the records that you determine not to be exempt.

NYCLU
ACLU of New York

We agree to compensate you for the cost of duplicating the records we request, as provided by law. Upon locating the requested documents, please contact us prior to photocopying and advise us of the actual costs of duplication so that we may decide whether a narrowing of the request will be necessary. To the extent that records are available in electronic format, we request that they be provided in that format.

Please send responsive records to:

Stefanie Coyle
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
scoyle@nyclu.org

Definitions and General Parameters:

This request applies to records created or obtained by the New York State Education Department ("NYSED") or any of its subsidiaries at or relating to any and all of its existing or proposed locations. This request refers to the Lockport City School District's ("Lockport" or the "District") proposed use of funds under the Smart Schools Bond Act ("SSBA") to purchase facial recognition technology (the "Proposal").

The term "record(s)" is to be construed in its broadest sense in accordance with New York FOIL to include anything upon which information is recorded, including all documents, papers, letters, email correspondence, maps, books, tapes, photographs, films, recordings or other material, and electronic records, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business.[33]

The request is limited to records created or obtained between **April 1, 2018 and the present**.

[33] N.Y. PUB. OFF. LAW § 86(4).

Specific Requests:

1. Any records reflecting NYSED's communications with:
    a. Any employee, contractor, or school board member of the Lockport City School District, including the September 20, 2019 letter described in NYSED's November 27, 2019 letter;
    b. Any employee, contractor, or board member of SN Technologies;
    c. J.A. "Tony" Olivo;
    d. Any employee, contractor, or board member of Corporate Screening and Investigative Group, LLC; and/or
    e. Any employee, contractor, or board member of Ferguson Electric Construction Company, Inc.
2. Any records reflecting NYSED's internal communications regarding biometric surveillance, facial recognition technology, or the Proposal;
3. Any records regarding the "privacy assessment" undertaken by NYSED with regard to Lockport's facial recognition system;
4. Any records reflecting invoices submitted by Lockport for reimbursement for its Smart Schools Bond Act proposals;
5. Any records reflecting accuracy tests and evaluations of Lockport's facial recognition technology and, if existing, on representative datasets, disaggregated by age, gender, and race;
6. Any records reflecting accuracy evaluations of the shape-based recognition system and descriptions of what testing data was used; and
7. Any 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 Proposal.