FACEOFF: THE FIGHT FOR PRIVACY IN AMERICAN PUBLIC SCHOOLS IN THE WAKE OF FACIAL RECOGNITION TECHNOLOGY

Alisia LoSardo

I. INTRODUCTION

In addition to parents, teachers, administrators, and coaches, a new set of eyes may soon be monitoring the children of the Lockport City School District ("Lockport" or "the District"). Last year, Lockport, located in western New York, announced that it was in the process of installing over 300 high-tech security cameras throughout their ten schools, all equipped

with Facial Recognition Technology ("FRT").[1] The District, using public funds granted to it by the Smart School Bond Act, originally proposed using nearly $3.3 million in order to fully implement the system.[2] Lockport expressed that this implementation is a response to the increasingly dangerous classroom environment that American children have been subjected to in recent years; the FRT system is meant to enable school security to quickly respond to the appearance of threats, such as registered sex offenders, disgruntled employees, expelled students, or persons carrying weapons.[3] Administrators believe that the system will be an effective means of thwarting serious threats like school shootings.[4]

While student safety is unquestionably of grave importance, Lockport's announcement was met with overwhelming backlash.[5] Most voiced similar concerns over Lockport's new system and the potential detrimental effects it may have on its students.[6] One Lockport father, Jim Shultz, expressed his disdain for the system in an article published by the New York Times, labeling Lockport's plan a "wasteful and dangerous experiment."[7]

---

* J.D. Candidate, 2020, Seton Hall University School of Law; B.A. in Psychology with a concentration in Behavioral Neuroscience, Fairfield University, May 2016. I would like to extend a special thank you to everyone involved in this comment, especially to my faculty advisor, Dean Brian Sheppard, and my Comment Editor Rakiah Bonjour. I would also like to thank my parents, Joseph and Rosemarie LoSardo, for their relentless love and support in everything I do.

[1] Thomas J. Prohaska, *NYCLU Attacks Lockport Schools' Facial Recognition Security Plan*, THE BUFFALO NEWS (April 4, 2019), https://buffalonews.com/2018/09/03/nyclu-attacks-lockport-schools-facial-recognition-security-plan.

[2] *See* President John Linderman, Lockport Board of Education Proceedings of the Board of Education Minutes (Aug. 17, 2016), https://www.nyclu.org/sites/default/files/field_documents/lockport_board_meeting.pdf [hereinafter Lockport Minutes]; Smart Schools Q & A, New York State Educ. Dep't. (2014) https://www.governor.ny.gov/sites/governor.ny.gov/files/archive/governor_files/documents/SmartSchools-QandA-9-15.pdf (The Smart Schools Bond Act authorizes the issuance of $2 billion to finance educational technology and infrastructure; spending must be approved by a state-wide vote before becoming effective. More recent reports indicate that Lockport has only moved forward with an initial implementation phase of $1.4 million thus far by installing the system); Kyle S. Mackie, *NYS Education Department Now "Satisfied" With Lockport City School's Facial Recognition Technology*, WBFO BUFFALO'S NPR NEWS STATION (Nov. 27, 2019), https://news.wbfo.org/post/nys-education-department-now-satisfied-lockport-city-schools-facial-recognition-technology.

[3] Associated Press, *Schools Using Facial Recognition Tech to Boost Safety*, N.Y. POST (July 23, 2018), https://nypost.com/2018/07/23/schools-using-facial-recognition-tech-to-boost-safety.

[4] *Id*.

[5] *E.g.*, Prohaska, *supra* note 1.

[6] Prohaska, *supra* note 1.

[7] Jim Shultz, *Spying on Children Won't Keep Them Safe*, THE NEW YORK TIMES (June 7, 2019), http://www.nytimes.com/2019/06/07/opinion/lockport-facial-recognition-schools.html.

Of these groups, however, the most vocal and effective has been the New York Civil Liberties Union ("NYCLU").[8] Just months after Lockport announced its plan, the NYCLU began working to have the New York State Education Department ("NYSED") withhold funding from the District in order to thwart the use of the technology completely.[9] The group also urged the District to reconsider, arguing that the system's implementation would create a host of social and privacy-related issues for its students.[10] The NYCLU asserted that not only would FRT violate the protected privacy and civil liberty rights of the students of Lockport, but it would also negatively impact their learning environment.[11] Socially, the organization asserted that the invasive nature of the surveillance would make students feel like criminals, decrease the leniency of minor offenses, and further the racial bias already prevalent in classrooms.[12]

Perhaps more concerning is that Lockport began installing the system without informing parents, students, or faculty members of any limitations, restrictions, or protocol that would accompany the system.[13] In her initial response, Lockport Superintendent Michele T. Bradley simply commented that all final protocols would be "guided by the interests of safety and security within the district and will be consistent with all applicable laws."[14] NYCLU spokeswoman Naomi Dann argued that Lockport should have been transparent from the outset regarding both how the technology would be implemented, and the steps that the District would take to ensure that privacy and civil liberty rights would be safeguarded.[15]

In addition to privacy concerns, Dann also stressed the need for protections against this sort of massive collection of data and the potential for it to be shared with law enforcement, immigration authorities, and other third-party agencies that may have an interest in obtaining such information.[16] The NYCLU warns that exposing children and faculty to such an invasive technology will create the possibility that "innocent students will be misidentified and punished for things that they did not do" and transform

---

[8] Letter from John A. Curr III, Western Reg. Office Dir. and Stefanie D. Coyle, Edu. Counsel, to MaryEllen Elia, NYS Edu. Dep. Commissioner, (June 18, 2018) (on file with author) (voicing the NYCLU's concerns regarding FRT in the Lockport schools and urging the District to cease their efforts).

[9] Prohaska, *supra* note 1, at 3.

[10] Prohaska, *supra* note 1, at 3.

[11] *See* Press Release, NYCLU, NYCLU Urges State to Block Facial Recognition Technology in Lockport Schools (June 18, 2018), https://www.nyclu.org/en/press-releases/nyclu-urges-state-block-facial-recognition-technology-lockport-schools.

[12] *Id*.

[13] Prohaska, *supra* note 1, at 3.

[14] Prohaska, *supra* note 1, at 3.

[15] Prohaska, *supra* note 1, at 3.

[16] Prohaska, *supra* note 1, at 3.

the school's environment from "one of learning and exploration into one of suspicion and control."[17] The NYCLU then filed a lengthy Freedom of Information Law ("FOIL") request with Lockport in order to generate material for its imminent report.[18]

The activism of parents and groups such as the NYCLU has led to some progress. Prior to the start of the 2019 school year, the NYSED delayed Lockport from fully implementing the system, requiring the District to make improvements and revisions to the protection of privacy in future collected data.[19] Lockport, however, remains determined to begin using the system at its full potential, indicating they will "continue to evaluate the timing for full implementation of the object and facial recognition components of the system."[20]

While the NYCLU's relentless advocacy of fully thwarting Lockport's plan has temporarily deterred the District, it is unlikely that it will ultimately prevent Lockport, or other schools throughout the country, from using such technologies. The NYCLU's main legal argument is that the use of FRT is a violation of the privacy rights of the students; however, under current jurisprudence, it is unlikely that FRT will infringe on a student's right to privacy.[21] Further, as current state and federal laws regarding biometric data collection are ill-equipped to protect *adults* from the nonconsensual use of FRT, they will undoubtedly be ineffective in protecting public school children, whose rights to privacy are substantially weakened.[22] While the NYCLU has put forth a convincing list of potential negative implications revolving around the technology, it would be far too one-sided to not also consider the potential benefits this system could provide its students.

---

17 Prohaska, *supra* note 1, at 3.

18 Prohaska, *supra* note 1, at 3.

19 Madison Carter, *I-Team: Lockport Schools Pull Faces From Facial Recognition System*; *Will Only Track Guns,* NEWS 7 ABC BUFFALO WKBK (Sept. 9, 2019, 6:21 PM), https://www.wkbw.com/news/i-team/i-team-lockport-schools-pull-faces-from-facial-recognition-system-will-only-track-guns (noting, presently, the system is only being used to monitor for guns).

20 Kyle S. Mackie, *NYS Education Department Now "Satisfied" with Lockport City Schools' Facial Recognition Technology*, WBFO88.7 (Nov. 27, 2019), https://news.wbfo.org/post/nys-education-department-now-satisfied-lockport-city-schools-facial-recognition-technology.

21 Press Release, *supra* note 11.

22 *See generally*, Sharon Nakar & Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy,* 23 B.U. J. SCI. & TECH. L. 88 (2017) (discussing facial recognition's ability to allow the government to track the movement of their citizenry in an "unprecedented fashion" and US courts' inability to protect individuals from being tracked).

This comment takes a moderate approach in joining the nuanced debate that currently exists around the implementation of FRT within the American public school system.[23] Though Lockport may be one of the first school districts fighting to implement FRT, it certainly will not be the last.[24] Recently, Seattle-based digital software company RealNetworks began offering a free version of its facial recognition system to schools nationwide.[25] Thus, as the implementation of this technology becomes more prevalent and readily accessible to schools, it is crucial that the federal government views Lockport as an opportunity to create stricter regulations revolving around FRT, and establish safeguards that protect the intimate data that is being collected.

Part II of this comment will provide a brief history of FRT; analyze FRT's origin, the manner in which it processes, stores, and collects biometric data; and evaluate the ways in which it is currently being used in schools. Part III attempts to balance the technology's prospective benefits with potential detrimental effects and abuses. Parts IV and V consider current jurisprudence in terms of student privacy rights, a school's duty to educate and protect its students, and federal policies that may protect collected student biometric data. Ultimately, this comment seeks to demonstrate the current lack of regulation and protocol that are applicable to this developing and invasive technology in public school systems. Further, it advocates for stricter federal regulations through amendments to preexisting federal laws, such as the Family Educational Rights and Privacy Act ("FERPA"), as a plausible solution to promote safety while ensuring a reasonable degree of privacy.

II. BACKGROUND

A. The Creation and Evolution of FRT

The notion of using one's facial composition in order to identify unknown suspects is one that dates back to the nineteenth century.[26] In essence, FRT is the natural evolution of centuries of law enforcement and governmental agencies expanding upon and attempting to perfect basic concepts of photo identification.[27] Though the general public's most prominent interaction with FRT may date back only a few years to Apple's

[23] This comment solely deals with FRT within public schools; private schools and the privacy rights of the faculty within the school systems are beyond the scope of this comment.

[24] Associated Press, *supra* note 3.

[25] Associated Press, *supra* note 3.

[26] MARCUS SMITH, MONIQUE MANN & GREGOR URBAS, BIOMETRICS, CRIME AND SECURITY 54 (Routledge 2018).

[27] *Id.*

novel use of the technology as a means of unlocking one's iPhone, efforts in the development of FRT have been continuously made since the 1960s.[28]

By the 1960s, technology had already been developed that could classify still photos of individuals by manually inputting measurements between facial features such as the eyes, nose, hairline, and mouth.[29] In the 1980s, algebraic techniques were then incorporated into the process so that FRT software required fewer than 100 measurements in order to effectively code a face.[30] Finally, a massive expansion of FRT in the U.S. occurred in the 1990s when the Defense Advanced Research Products Agency ("DARPA") sponsored The FacE REcognition Technology Evaluation ("FERET") in order to ultimately propel the technology from infancy into the commercial market.[31] Today, FRT is used widely by commercial entities in both the private and public sectors.[32] The U.S. government uses the technology extensively in various sectors as a means to promote safety.[33] For example, FRT can be used as a means to combat passport fraud in airports, to support law enforcement in uncovering the identity of missing children, and to minimize identity fraud.[34]

Essentially, most FRT software boils down to two fundamental processes: enrollment and matching.[35] Most algorithms divide the face into distinctive nodal points that are individual to a person and will change minimally over time.[36] FRT seeks out patterns using features such as eye sockets, nose shape, distances between unique features (like moles, spots, or glasses), skin texture, and weighted areas of the face.[37] Collecting and imputing these data points is known as the enrollment phase, and it creates a digital "faceprint."[38] Next, FRT software compares this data to a preexisting database full of other facial models in order to identify an individual.[39] The data collected in order to create these faceprints are a type of biometric data. Biometric data, most simply, refers to any "measurement of a physical

---

28 KELLY GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE, 27, (New York University Press, 2011).

29 Jesse D. West, *A Brief History of Face Recognition*, FACEFIRST (Aug. 1, 2017), https://www.facefirst.com/blog/brief-history-of-face-recognition-software.

30 *Id.*

31 *Id*.

32 *See generally id*.

33 *Id.*

34 FEDERAL BUREAU OF INVESTIGATION, SUBCOMMITTEE ON BIOMETRICS, FACE RECOGNITION 93 (2014). [hereinafter FBI Biometrics]

35 SMITH ET AL., *supra* note 26, at 7.

36 SMITH ET AL., *supra* note 26, at 7.

37 Nakar, *supra* note 22, at 95.

38 Nakar, *supra* note 22, at 95.

39 Nakar, *supra* note 22, at 95.

feature of the human body."[40] Further, first generation biometrics relate to physiological data, such as fingerprints and facial recognition, whereas second generation biometrics have gone even further and are able to identify an individual based on behavioral patterns such as gait, keystroke analysis, and cognitive function.[41] In order to successfully identify an individual, the biometric data collected must be a "measurable, robust and distinctive physical characteristic or personal trait."[42]

Lastly, and particularly important to its application to schools, FRT serves two basic functions: verification and identification.[43] Verification works by using the technology in a one-to-one matching fashion.[44] This, for example, is the process that the iPhone undergoes in order to unlock; once it detects the owner's specific and stored faceprint, it opens. Identification, on the other hand, occurs through a one-to-many search, where large databases are searched for a similar facial template to render a match.[45] Thus, though Lockport has yet to introduce any set of protocols for their program, the system could potentially store any number of faceprints and program the building to only open certain doors upon verification, or uncover the identities of those who have committed minor offenses or crimes in the building.[46]

Though the average individual may not believe that they have much experience with FRT outside of the commercial realm, the odds that they have been participants in a governmental FRT, albeit unknown and nonconsensual, are quite high.[47] For example, the New York Department of Motor Vehicles has implemented an enhanced FRT system that already holds over 16 million photos in its database as a means of combatting identity theft and fraud.[48] Additionally, police departments across the country have adopted FRT software in order to pursue and prosecute prostitutes, drug dealers, and other non-violent offenders.[49] In fact, it has been estimated that FRT searches apply to more than 117 million American adults; a number that is continuously growing.[50] This equates to approximately half of the

40 SMITH ET AL., *supra* note 26, at 2.
41 SMITH ET AL., *supra* note 26, at 2.
42 SMITH ET AL., *supra* note 26, at 2.
43 SMITH ET AL., *supra* note 26, at 56.
44 SMITH ET AL., *supra* note 26, at 56.
45 SMITH ET AL., *supra* note 26, at 56.
46 *See generally,* Associated Press, *supra* note 3.
47 *See generally* Nakar, *supra* note 22.
48 *See* Nakar, *supra* note 22, at 90.
49 *See* Nakar, *supra* note 22, at 97.
50 Georgetown Law, *Half of All American Adults are in a Police Face Recognition Database, New Report Finds* (Oct. 18, 2016), GEORGETOWN LAW, https://www.law.georgetown.edu/news/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds.

adults in America having their photo identification in a facial recognition database.[51]

B. Biometric Data Collection in American Schools

While the introduction of FRT into schools is entirely novel, the collection of student biometric data is not. As early as 2000, for example, Minnesota's Eagan High School was using fingerprinting to manage the accounts of students borrowing books from its library.[52] By 2013, a number of schools reported using iris scans in lieu of traditional school IDs as a way for students to "check in" when boarding school buses.[53] The use of technology as a means to monitor students became so prevalent that by 2013–14, 75% of all K-12 schools in the U.S. began using security cameras.[54] In 2016, it was estimated that the collection of some form of biometric data, including fingerprinting, iris scans, palm scans, and radio frequency identification, was being collected from students in more than 1,000 school districts in forty states throughout the U.S.[55] In response to criticism of these techniques, most districts have recognized that, though a tradeoff of student privacy for efficiency and safety does exist, it is one worth making in the face of the unprecedented rates of terroristic threats and attacks in American schools.[56]

As introduced at the start of this comment, the most recent and certainly the most aggressive development in the collection of student biometric data is currently unfolding in Lockport.[57] On August 17, 2016, at the proceeding of the Board of Education, Lockport announced its proposal to use public funds to "upgrade" their current security cameras through SN Technologies.[58] SN Technologies is a private, Ontario-based technology company that produces security systems specifically designed for school

---

51 *Id.*

52 Haydn Evan, *The State of Biometric Technology: The Uses, The Concerns,* LAW 360 (August 8, 2017) https://www.law360.com/articles/950365/the-state-of-biometrics-technology-the-uses-the-concerns.

53 Stefan P. Schropp, *Biometric Data Collection and RFID Tracking in Schools: A Reasoned Approach to Reasonable Expectations of Privacy*, 94 N.C.L. REV. 1068, 1073-74 (2016) (citing Laurie Segall & Erika Fink, *Iris Scans Are the New School IDs,* CNN MONEY (July 11, 2013), http://money.cnn.com/2013/07/11/technology/security/iris-scanning-school).

54 J. William Tucker & Amelia Vance, *School Surveillance; The Consequences for Equity and Privacy*, 2 EDUCATION LEADERS REPORT 4, 3 (Oct. 2016) (citing a report conducted by the U.S. DEPARTMENT OF EDUCATION, NATIONAL CENTER FOR EDUCATION STATISTICS, PUBLIC SCHOOL SAFETY AND DISCIPLINE: 2013-2014 (2015)).

55 Schropp, *supra* note 53, at 1068.

56 *See* Schropp, *supra* note 53, at 1092.

57 Lockport Minutes, *supra* note 2.

58 Lockport Minutes, *supra* note 2.

security.[59] Their mission is to use facial, shape, and pattern recognition technology specifically designed for the school sector to protect students and staff on school property.[60] The system that the company uses in order to carry out this mission consists of three main functions: (1) it uses FRT to detect unwanted individuals (suspended students, fired employees, known gang members, those on the local sex offender registry, or other dangerous individuals that can be programed into the system); (2) it has the ability to detect gun shapes; and (3) it can review previously recorded videos in search of specific individuals.[61]

Michael Vance, a representative of SN Technologies, addressed concerns about the new system's use in Lockport by stating that the images and biometric data that is collected will reside and remain with the schools.[62] He assured those that expressed concerns the company does not "see" the collected data: "[w]e don't have access to the pictures, the video, anything like that. It's stored in the same way that school attendance databases, grades, records, everything is kept."[63] In terms of the potential for data to be shared with other public entities, school security consultant Tony Olivo stated, "The extent to which any security camera data will be shared with law enforcement agencies will be addressed in the final protocols, which will be guided by the interests of safety and security within the district and will be consistent with all applicable laws."[64] Lockport has stressed that they have used a surveillance system in their schools for over a decade and that the FRT is no more than a mere "upgrade" to their current system, one that will do nothing but further safeguard students against potential threats.[65]

Moreover, the fact that emerging technology companies such as RealNetworks will begin offering free FRT systems to school districts nationwide, in combination with the inevitability that such technology will continue to develop and become more sophisticated and intrusive, furthers the need to critically analyze the potential harms that may accompany it.

III. BALANCING POTENTIAL HARMS AND BENEFITS

Children need to feel safe in order to thrive in the classroom.[66] Studies conducted on K-12 students found that those who feel safe while in class

---

59 Associated Press, *supra* note 3.

60 *See* SN TECHNOLOGIES, http://www.sntechnologies.ca/product (last visited Jan. 16, 2020).

61 *Id*.

62 Associated Press, *supra* note 3.

63 Associated Press, *supra* note 3.

64 Prohaska, *supra* note 1.

65 Associated Press, *supra* note 3.

66 Tucker & Vance, *supra* note 54, at 5.

"have higher attendance rates, better academic performance, and may experience fewer classroom disruptions than other students."[67] Conversely, the effect of over-surveillance on learning has also been well-studied; findings of which demonstrate that it is accompanied by its own set of detrimental effects.[68] The introduction of FRT not only increases the severity of previous surveillance concerns, but exposes students to a whole new host of privacy and data harms as well. It is critical to balance such harms with the potential benefits in order to fairly assess the implementation of such a novel technology.

A. Benefits: The Increasing Need for Safety in America's Schools

While adverse effects promulgated by organizations such as the NYCLU seem daunting, it is important to remember that they are merely predictions of what schoolwide FRT implementation may yield. It would be irresponsible to not also recognize that FRT, if accompanied by the proper guidelines and limitations, has the potential to promote safety and efficiency for students. In the public sector, FRT is cited by agencies such as the FBI as an effective tool used to thwart crime.[69] For example, FRT has been effectively utilized by authority in order to track and capture terrorists, convict participants of prostitution, break up drug rings and locate missing persons.[70]

In light of the increasing severity of violence that threatens students and faculty, FRT may ultimately prove to be beneficial as moderate levels of surveillance are "essential for the public good."[71] Private FRT companies that market their systems to school districts, such as RealNetworks and SN Technologies, advertise that the safety implications would be immense.[72] RealNetworks alleges that the technology would ensure that doors remain locked for individuals that are not programmed into the system, thus decreasing the overall likelihood that unwanted or dangerous individuals find their way in.[73] The company also asserts that the system can be programmed to detect dangerous objects such as guns or other weapons.[74] Finally, they claim that all facial data and images are encrypted to ensure

67 Tucker & Vance, *supra* note 54, at 7.

68 *See* Tucker & Vance, *supra* note 54, at 9.

69 FBI Biometrics, *supra* note 34 at 93.

70 FBI Biometrics, *supra* note 34 at 93; Nakar, *supra* note 22, at 97.

71 DAVID WRIGHT & REINHARD KRESSL, SURVEILLANCE IN EUROPE 328 (David Wright & Reinhard Kressl eds., 2015).

72 SN TECHNOLOGIES, *supra* note 60; REAL NETWORKS, *Safr for K-12 Schools*, https://safr.com/k12 (last visited Jan. 16, 2020).

73 Webinar: Enhance School Safety with Secure, Accurate Facial Recognition (Real Networks 2018) (available at https://safr.com/k12).

74 *Id*.

privacy and that no images or data are ever transmitted over the internet.[75]

Technology companies and the school districts to which they market seem to feel confident that they can ensure privacy while increasing safety and efficiency.[76] However, identifying and analyzing the many harms and concerns of FRT is a crucial first step in ensuring that the appropriate measures be taken.

B. Harms; Social implications and Privacy Concerns

1. Normalizing Privacy Invasions and the "Surveillance Effect"

One of the most alarming implications of FRT is the concern that it will normalize invasive means of surveillance in the eyes of students at a very young age.[77] Experts have argued that the technology will breed a "generation that will be comfortable with and fully accepting of total government surveillance."[78] The idea of constant surveillance will likely have immense ramifications on the way students think about privacy and the government's place in monitoring behavior in the interest of safety.[79] If students are made to feel that authority figures essentially have a right to continuously monitor their actions, whether in a private place or not, it could normalize that notion as they enter adulthood.

Another major concern with the implementation of FRT is a concept widely-known as the "surveillance effect."[80] The surveillance effect has been well-researched in American school systems since the emergence of security cameras as a means of monitoring K-12 students.[81] The main notion is that students who feel as though they are being constantly watched will feel that they are in a "less nurturing, comfortable learning environment."[82] Further, the surveillance-effect theorizes that the result of such a feeling interferes with the development of a sense of trust and cooperation at school between the students and the administration/faculty.[83] Students that have been exposed to school climates that involve the extensive use of metal detectors, uniformed security guards, and surveillance cameras have shared

---

75 *Id*.

76 *See e.g*., SN TECHNOLOGIES, *supra* note 60.

77 *See generally*, Tucker & Vance, *supra* note 54.

78 Brian Heaton, *State Legislatures Grapple with Biometrics Use in Schools*, GOVTECH TODAY (April 5, 2019), https://www.govtech.com/State-Legislatures-Grappling-with-Biometrics-Use-in-Schools.html.

79 *Id*.

80 Tucker & Vance, *supra* note 54, at 8.

81 Tucker & Vance, *supra* note 54, at 7.

82 Tucker & Vance, *supra* note 54, at 8.

83 Tucker & Vance, *supra* note 54, at 8.

their experiences about their interactions with such technology.[84] Edward Ward, a student exposed to such an environment while attending high school in Chicago's West Side recounted, "[f]rom the moment we stepped through the doors in the morning, we were faced with metal detectors, x-ray machines, and uniformed security guards. . . . I could slowly see the determination to get an education fade from the faces of my peers because they were convinced, they no longer mattered."[85]

Feelings of apathy witnessed by Ward will likely intensify with the addition of FRT into existing security cameras within schools that are already heavily monitored. In addition to the general notion that they are being watched, students may also come to understand that their cameras have the capability to recognize *who* they are and specifically track them if deemed warranted. For example, if a student has a history of misbehaving, the FRT software can keep an eye on him or her specifically throughout the school day in order to ensure obedience.[86]

The ability to track individual students may also lead to a heightened penalization of minor offenses that would have otherwise gone unnoticed.[87] This is problematic because educational environments are meant to be spaces that facilitate growth and change among adolescents.[88] It has been widely accepted that a certain degree of leniency and a small "margin of error" should generally be awarded to students, most of whom are grappling with their own sense of identity and simply striving to fit in with those around them.[89] As adults, we recognize that children and teenagers are going to make mistakes; in fact, it is critical to their development and ability to mature.[90] Experts argue that schools should remain, as they have always been, facilities of "human growth and development."[91] The existence of FRT and surveillance cameras fail to promote the notion of "forgiving and forgetting," making students feel as though their minor misconducts will inevitably come back to haunt them.[92] American schools have typically valued environments that ensure positive growth and change, even if through mistakes; therefore, the use of FRT in schools will likely erode these

84 Tucker & Vance, *supra* note 54, at 9.

85 Tucker & Vance, *supra* note 54, at 9 (citing Edward Ward, a DePaul University honor roll student, who shared his experience on the detrimental effects of over-surveillance growing up in one of the most heavily monitored schools in Chicago's West Side).

86 *See generally*, Press Release, *supra* note 11.

87 Tucker & Vance, *supra* note 54, at 12.

88 Tucker & Vance, *supra* note 54, at 9.

89 *Generally*, Tucker & Vance, *supra* note 54, at 8.

90 Tucker & Vance, *supra* note 54, at 9.

91 Tucker & Vance, *supra* note 54, at 9.

92 Tucker & Vance, *supra* note 54, at 12.

fundamental concepts.[93]

2. A Threat to Intellectual Privacy and Expression

Additionally, FRT has the potential to infringe on intellectual privacy.[94] Experts in education have stressed that "[i]ntellectual privacy is the much-needed protection for learning, reading and communicating that helps us make up our minds about the world on our own terms."[95] Intellectual privacy exists when students feel that they can express their thoughts, feelings, and ideas without feeling as though they are being watched or judged.[96] When students feel they cannot express their thoughts and ideas, or when they feel their ideas may be recorded and stored, their thoughts and beliefs "get driven to boring, [to] the bland and the mainstream."[97] If a student is aware of the possibility that whatever they are saying or doing could theoretically be recorded and shared, it is quite likely that their creativity, risk-taking, and overall inquisitiveness will decrease while they are inside the classroom.[98]

3. The Faultiness of FRT

Another concern about implementing FRT is the fact that, though the technology has been around for decades, it is still largely in its infancy and the accuracy of systems similar to Lockport's remains unknown. For example, just last year, the South Whales Police Department released the results of an experiment that displayed the potentially immense shortcomings of FRT.[99] At the Champions League's final game, the police used FRT to log the identities of fans in the stadium; their system correctly logged 173 faces and wrongly identified 2,297 individuals.[100] The system falsely identified approximately 92% of the participants.[101] The police department defended the system, stating that it was created with the intention of locating one individual in a crowd rather than matching identities of the masses.[102] The department also stated that it is continuing to improve upon

93 Tucker & Vance, *supra* note 54, at 9.

94 Tucker & Vance, *supra* note 54, at 9.

95 Neil Schoenherr, *Intellectual Privacy Vital to Life in the Digital Age*, THE SOURCE (Feb. 2, 2015), https://source.wustl.edu/2015/02/intellectual-privacy-vital-to-life-in-the-digital-age (citing Neil Richards, member of the Advisory Board of the Future of Privacy Forum and a consult and expert in privacy law).

96 Tucker & Vance, *supra* note 54, at 9.

97 Tucker & Vance, *supra* note 54, at 9.

98 Tucker & Vance, *supra* note 54, at 9.

99 Lily H. Newman, *Facial Recognition Tech is Creepy when it Works and Creepier when it Doesn't,* WIRED (May 9, 2018), https://www.wired.com/story/facial-recognition-tech-creepy-works-or-not.

100 *Id*.

101 *Id*.

102 *Id*.

the system's overall accuracy.[103] Nonetheless, the overwhelming number of false-positives that occurred is worrisome.

Additionally, current systems have been known to generate false-positives when an individual makes even minor aesthetic changes.[104] For example, changes in hair, glasses, facial hair, and headscarves have been shown to "fool" the system.[105] As K-12 children are likely to go through a plethora of different styles and natural physical changes, this will likely interfere with the system and has the potential to find innocent children at fault for acts that they may not have committed.

Discrimination against people of color and women has also been explored in current FRT systems.[106] Ethnic minorities are subject to a greater risk of inaccuracy due to the fact that many algorithms that compare facial templates skew or influence the types that are identified based on the databases that they are pulling from.[107] For example, some programs draw from police databases that contain a disproportionate number of black and minority individuals.[108] Further, there is already a racial disparity that exists in the classroom.[109] Those who oppose the system worry that this technology has the potential to negatively affect, and unnecessarily worry students who come from immigrant backgrounds because of the possibility of data sharing with services such as immigration and customs enforcement.[110]

4. Data Collection

Finally, a major concern revolves around data management. The biometric information taken from children exposed to FRT is highly sensitive. If a student attends Lockport from K-12, the school will essentially have a faceprint of that child at each stage of their development. Moreover, once the child is around eighteen, though they will naturally continue to develop, measurements such as their nose length, the space between their eyes and other biometric measurements are not likely to change. If these biometric measurements are shared with government agencies and other third parties, they have the capability to be used as a virtual tracking device. Commercial threats and student data unknowingly being sold to third parties

103 *Id*.

104 SMITH ET AL., *supra* note 26, at 64.

105 SMITH ET AL., *supra* note 26, at 64.

106 SMITH ET AL., *supra* note 26, at 64.

107 SMITH ET AL., *supra* note 26, at 65.

108 SMITH ET AL., *supra* note 26, at 65.

109 Ava Kofman, *Face Recognition is Now Being Used in Schools, but it won't Stop Mass Shooting,* THE INTERCEPT (May 30, 2018), https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings.

110 *Id.*

are just a few examples of how problematic this technology can become.[111]

In light of all of these potential harms, the NYCLU has advocated for a complete rejection of FRT in schools.[112] Others have agreed: "Imagine a technology that is so potently, uniquely dangerous . . . something so pernicious that regulation cannot adequately protect citizens from its effects."[113] The outcry from prominent groups such as the NYCLU and privacy experts alike should signal schools to proceed with great caution when considering the implementation of FRT, especially to provide safeguards necessary to protect students against its many projected, yet ultimately unknown harms.

IV. STUDENT PRIVACY RIGHTS IN THE FACE OF FRT

In an attempt to completely prevent these potential harms and the use of any FRT in Lockport, one of the major arguments that the NYCLU relies upon is the notion that the technology will infringe on the privacy rights of students.[114] However, an analysis of recent Supreme Court decisions and state and federal regulations reveal an alarming lack of protection.

A. Privacy Case Law

It is unlikely that the use of FRT will be considered a violation of a student's right to privacy under current Supreme Court jurisprudence. Though the Court has never faced this question head-on, an analysis of FRT cases read in conjunction with student privacy rights cases provides an appropriate framework.

The Fourth Amendment, in its most basic sense, is meant to promote individual privacy by prohibiting the government from conducting unreasonable searches and seizures.[115] A few prominent Supreme Court

---

111 The collection of biometric data and potential for commercial misuse has been written on extensively and a full discussion of it is outside the scope of this note. *See e.g.*, Alex Molnar, Faith Boninger & Ken M. Libby, *Schoolhouse Commercialism Leaves Policymakers Behind*, NAT'L EDUC. POLICY CTR. (2014), http://nepc.colorado.edu/files/trends-2013.pdf.

112 Press Release, *supra* note 11.

113 Evan Selinger and Woodrow Hartzog, *Professors Evan Selinger and Woodrow Hartzog Disclose the Privacy Risks of Facial Recognition,* TAP, (July 5, 2018), https://www.techpolicy.com/Blog/July-2018/Professors-Evan-Selinger-and-Woodrow-Hartzog-Discl.aspx; *Facial Recognition Technology: Ensuring Transparency in Government Use: Statement for the Record Before the H. Oversight and Reform Committee*, 116th Cong. (2019) (statement by Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Division, Federal Bureau of Investigation). As previously stated, this comment only very briefly touches on the issues associated with the data collection of school children. For a more in-depth discussion, *see e.g.,* Schropp, *supra* note 53.

114 Curr, *supra* note 8 (advocating the NYCLU's concerns regarding FRT in the Lockport schools and urging the District to cease their efforts).

115 Tucker & Vance, *supra* note 54, at 10; U. S. CONST. amend. IV.

cases have addressed this right as it pertains to technology such as surveillance cameras, and a number of experts have drawn implications as to what an average citizen's rights are in the wake of FRT.[116] A monumental case in the realm of privacy is *Katz v. United States*.[117] In *Katz*, a Supreme Court case that questioned the constitutionality of wire taps placed in phone booths, the Court held that the Fourth Amendment protects people, rather than areas, against unreasonable searches and seizures.[118] In a recent summary of the law, the Arizona Court of Appeals noted that, "even in the absence of trespass, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[119] The Court summarized that the search is deemed constitutional unless an individual exhibits an expectation of privacy *and* that expectation is one that society is willing to recognize as reasonable.[120]

The court further illustrated this point in *People v. Johnson,*[121] a California case that addressed the admissibility of FRT as evidence of identifying a guilty party.[122] In *Johnson*, the court stated that, for trial purposes, whether FRT was used to identify an individual is ultimately irrelevant; the court viewed FRT as merely a database that provides law enforcement with an investigative tool.[123] In most contexts, FRT takes place in areas and situations wherein the individual has little to no expectation of privacy such as open public spaces or street corners.[124] The court then gave an example of a situation where a police unit uses FRT in order to capture a bank robber by comparing images of his face at the bank to images stored in a Department of Motor Vehicles ("DMV") database.[125] In this example, the means of initial identification by FRT occurred in a public space where an individual is certainly not afforded a reasonable expectation of privacy.[126] The court found the use of FRT essentially irrelevant so long as subsequent police protocols confirm the suspect.[127] The case also suggests that courts recognize the faultiness of FRT, commenting that it matters not to their

116 Tucker & Vance, *supra* note 54, at 10.
117 Katz v. United States, 389 U.S. 347 (1967).
118 *Id.* at 351.
119 Nakar, *supra* note 22 (citing State v. Estrella, 286 P.3d 150, 153 (Ariz. Ct. App. 2012)).
120 Nakar, *supra* note 22.
121 People v. Johnson, 43 Cal. Rptr. 3d 587, 597 (Cal. Ct. App. 2006).
122 Nakar, *supra* note 22; *see also id.*
123 *Johnson*, 43 Cal. Rptr. 3d at 597.
124 *Id*.
125 *Id*.
126 *Id*.
127 *Id*.

analysis whether "facial recognition software is discerning and accurate enough to select the perpetrator."[128] Ultimately, though not explicitly stated, it appears the use of FRT does not run afoul to the Constitution in public settings.

Children also enjoy a right to privacy, however, their rights as incorporated by the Fourteenth Amendment are significantly lessened in the public school setting.[129] In school settings, privacy protections are modified not only to impose responsibility on schools to keep children safe, but also schools have a legal duty to do so.[130] The Supreme Court has indicated that public schools have a "custodial and tutelary responsibility" for the children that attend them and that such responsibilities cannot be disregarded or taken lightly.[131] Additionally, Supreme Court cases over time have seemingly weakened the Fourth Amendment rights held by students.[132]

In *Brannum v. Overton County School Board*,[133] a case that will likely impact the use of FRT in schools, the Sixth Circuit specified reasonableness as it pertains to student searches conducted by surveillance cameras.[134] In order to determine whether school searches are constitutionally reasonable, courts engage in a fact-specific balancing test.[135] The *Brannum* Court balanced: (1) the government's need to conduct the search against; (2) the nature of the invasion that the search entails; and (3) student's reasonable expectation of privacy.[136]

Specifically, *Brannum* questioned whether or not the use of surveillance cameras placed in locker rooms violated a student's Constitutional right to privacy.[137] Ultimately, the court held that cameras placed in non-public locations—areas such as locker rooms where students have a reasonable expectation of privacy—violate the Fourth Amendment.[138] Further, in order to determine which spaces are protected, the case established a three-part framework: (1) the scope of legitimate expectation of privacy; (2) the character of the intrusion; and, (3) the nature and immediacy of governmental concern and the efficacy of the means employed for dealing with it.[139]

---

128 *Id*.
129 Schropp, *supra* note 53, at 1083-84.
130 Schropp, *supra* note 53, at 1083-84.
131 *See e.g.*, Veronia School Dist. 47J v. Action, 515 U.S. 646, 656 (1995).
132 Schropp *supra* 53, at 1077.
133 Brannum v. Overton County School Board, 516 F.3d 489 (6th Cir. 2008).
134 *See id.* at 497.
135 *See id.* at 496.
136 *Id*.
137 *Id*. at 491-92.
138 *Id*. at 497.
139 *Brannum*, 516 F.3d at 496.

Using this same three-part framework, it is likely that a court faced with the question of whether FRT's use in schools violates a student's privacy right would hold that in most areas it does not. In terms of the first element, a legitimate expectation of privacy, Lockport made it clear that the cameras are simply "upgrades" to their already-existing security camera.[140] Thus, it is unlikely that the cameras will be moved to or placed in areas where students have an expectation of privacy, such as a restroom or a locker room. If the school's cameras exist in hallways, lecture halls, and around exits and entrances, there will be no issue as to the first element.

The second element, character of intrusion, is the prong that may potentially weaken a school's ability to implement FRT under this standard. As FRT has yet to be used in a school context, its nature is difficult to define. FRT, and the biometric data that it collects, increases the severity of the intrusion. Now, not only are schools collecting images of their students, but those images are being collected, stored, and analyzed.[141] Courts may view FRT as a simple technological upgrade to security cameras and find it reasonable. On the other hand, due to its novel ability to store and preserve biometric student data, a court may find it an unreasonable means of promoting safety. In *Brannum*, the court provides guidance as to what constitutes a "justifiably intrusive search in light of purpose."[142] The court states that it finds the nature of video surveillance inherently intrusive; however, policies that the school put into action ensured that this intrusion was as minimally invasive as possible.[143]

Finally, with respect to the third element, the nature and immediacy of governmental concern, schools such as Lockport have provided a sound rationale for FRT implementation as a means to combat violence in schools, which has dramatically increased in recent years.[144] Schools will likely argue that the purpose of FRT, though it gathers highly sensitive data, is one of immediate concern because it is one of the newest ways to thwart attacks.

The *Brannum* Court also held that "as the commonly understood expectation of privacy increases, the range and nature of permissible governmental intrusion decreased."[145] Using this logic, the pervasiveness of modern technology amongst younger generations will likely cause privacy

---

140 *See* Lockport Minutes, *supra* note 2.

141 *Supra* notes 1-2.

142 *Brannum*, 516 F.3d at 496.

143 *Id.* at 497.

144 *See* Andrea Page, *Center for Homeland Defense and Security Releases Comprehensive Database of School Shootings in America*, HOMELAND SECURITY DIGITAL LIBRARY, (last visited Jan. 12, 2020), https://www.hsdl.org/c/database-of-school-shootings-in-america (reporting that 1,300 school shootings have occurred in America's K-12 schools since 1970).

145 *Brannum*, 516 F.3d at 498.

expectations to diminish, inversely causing FRT's range to increase and the nature of its function to gain acceptance. Other means of biometric data collection have been practiced routinely by schools for decades, as outlined above.[146] In terms of data collection and identification, fingerprint and iris scans may be considered on par with the collection of facial nodal points.[147] Due to the fact that it is unlikely that students will receive any protection from FRT under Constitutional law, it is necessary to look to federal and state regulation.

B. State Regulations

Although FRT is becoming increasingly prevalent in nearly all arenas of public life, few state laws currently regulate its use.[148] Recently, however, a number of states have addressed the biometric data collection component of such technology in schools.[149] For example, statutes in Illinois and Louisiana both "require that school systems receive permission" before collecting any biometric data; if the student is of legal age they must consent, and if the child is a minor, a parent must grant the school permission.[150]

The Illinois statute defines biometric information as "any information that is collected through an identification process for individuals based on their unique behavioral or physiological characteristics, including fingerprint, hand geometry, voice, or facial recognition or iris or retinal scans."[151] The statute provides that school districts that intend to collect these forms of data must "adopt policies that require, at a minimum, all of the following: written permission from the individual who has legal custody of the student. . . or from the student if he or she has reached the age of 18."[152] Similarly, the Louisiana law provides that administrations of each public elementary and secondary school that collects biometric information from students, "develop, adopt, and implement policies governing the collection and use of such information that, at a minimum, shall: require written permission from the student's parent or other legal guardian, or the student if he or she is eighteen years of age or older."[153]

Apart from biometric data collection, certain areas of the country have taken a determinative stance against the use of FRT in the public section at

146 *Supra* notes 52-55.

147 Schropp, *supra* note 53.

148 *See* Heaton, *supra* note 78 .

149 Tiffany Lee, *Biometrics and Disability Rights: Legal Compliance in Biometric Identification Programs,* 2016 U.ILL. J.L. TECH & POL'Y 209, 225 (2016).

150 *Id*. at 224-25.

151 *Id.* at 225 n.119.

152 *Id*.

153 *Id*. at 225 n.120.

large. Recently, San Francisco barred its police departments from using FRT software, joining two other cities, Oakland, California, and Somerville, Massachusetts.[154] The New York Legislature has indicated that they are now considering a similar ban through the proposal of bill that will be reintroduced next year.[155] The bill, sponsored by Monica P. Wallace, D-Lancaster, would also impose a three-year moratorium on the use of FRT in schools until the NYSED completes a thorough study on the topic.[156]

One solution in attempting to protect the privacy rights of children would be for other states to take notice of these few states, follow their lead, and perhaps expand upon the sentiments of their laws and proposed laws. A more uniform and comprehensive solution to the problem, however, may exist in federal regulation.

C. Federal Regulations

The federal statutes that are cognizably applicable to FRT in schools and carry the potential for regulation include The Family Educational Rights and Privacy Act ("FERPA"), The Children's Online Privacy Protection Act ("COPPA"), and The Protection of Pupil Rights Amendment ("PPRA"). Understanding how FERPA, COPPA, and the PPRA have developed and currently operate provides a better understanding of the shortcomings that exist and the need for stricter regulation.[157]

Advocacy for amending these policies is not a new notion. Policy makers at the highest level have taken note of the increasing tension that exists between the advancement of technology in the classroom and privacy, and civil liberty concerns.[158] In 2014, for example, a White House Report urged Congress to "modernize the privacy regulatory framework under [FERPA] and [COPPA]" to combat data sharing and misuse while still allowing school technology and innovation to flourish.[159]

The growing role of business in education is primarily responsible for this concern.[160] It is widely acknowledged that "activities considered commercial . . . by some could be viewed as part of the adaptive learning

---

154 Thomas Prohaska, *Lockport schools push to activate contentious facial recognition security system*, THE BUFFALO NEWS (Aug. 10, 2019), https://buffalonews.com/2019/08/10/despite-opposition-lockport-school-leaders-push-for-facial-recognition-security-system.

155 *Id.*

156 *Id*.

157 Jules Polonetsky & Omer Tene, *Who is Reading Whom Now: Privacy in Education from Books to MOOCs,* 17 VAND. J. ENT. & TECH. L. 927, 959 (2014).

158 *Id.* at 932.

159 *Id*. at 932 (citation omitted).

160 *Id.* at 949.

experience by others."[161] Even assuming the best of intentions, it is clear that market players are struggling to correctly balance commercial interests with student privacy rights.[162] FRT deepens these concerns, as the private companies that provide the technology would be in possession of highly sensitive biometric data.

In a slightly different vein, another overall area of weakness in these statutes is parental involvement; while the statutes are beneficial in requiring parental awareness, the average parent is often ill-positioned to take on such a task.[163] Specifically, asking parents to consider and examine the details of such a system would likely do very little for both the privacy and data protection of their child.[164]

The "opt-out" provisions of these statutes pose another problem in the face of FRT: when students and parents can "opt-out," a "duplicative system" is essentially created.[165] The school must then divide the technology amongst children who are able to enter and those who are not. If this were to happen in the context of what Lockport is attempting to do, a duplicative system's existence would completely thwart the entire purpose of the FRT cameras. That is, Lockport's system only works to identify threatening individuals when all faces are eligible to be scanned and compared to the school's preexisting database.

1. COPPA

COPPA's provisions exist solely to ensure that commercial companies obtain express parental consent prior to collecting children's (under the age of thirteen) information while online.[166] The statute plainly applies to commercial websites, online services directed at children, and websites and services that have actual knowledge that they collect personal information from children.[167] An important provision of COPPA, however, is that schools retain the right to consent in lieu of a parent.[168] Thus, while on its face the statute looks as though it may offer some form of protection as to FRT, it would be largely ineffective. First, it would only have the potential to protect children under the age of 13, leaving a number of K-12 students unprotected. Second, a school that is implementing the technology could simply consent to the data collection nullifying any potential protection.

161 *Id.* at 952.
162 *Id.* at 953.
163 Polonetsky & Tene, *supra* note 157, at 957.
164 Polonetsky & Tene, *supra* note 157, at 957.
165 Polonetsky & Tene, *supra* note 157, at 957.
166 Polonetsky & Tene, *supra* note 157, at 970.
167 Polonetsky & Tene, *supra* note 157, at 970.
168 Polonetsky & Tene, *supra* note 157, at 970.

2. PPRA

Alternatively, the PPRA's restrictions apply to school and third-party uses of student data to marketing explicitly.[169] The PPRA requires school districts to notify parents in cases of collection, disclosure, use, or sale of student information for marketing purposes, and provides parents with the opportunity to opt their child out of such uses.[170] Further, the statute applies to information that reveals "political affiliation, mental and psychological concerns, sex behaviors, and income."[171] Primarily, the PPRA was created in order to safeguard survey-like information collected at school from marketing purposes; it is unlikely that the PPRA would protect the disclosure of student biometric data from being shared with governmental agencies such as law enforcement and immigration agencies.[172]

3. FERPA

The most applicable of these three statutes is FERPA. Passed in 1974, FERPA was created because prior to its existence, it was not clear which parties had access to student data and what rights parents had to their own child's collected information.[173] For example, a story praising a student for an athletic achievement could be easily published in the paper and list his or her weight, height, grades, and include a photograph of them for the general public to access without any consent granted from a parent or the student themselves.[174] Additionally, it was relatively easy for police and health departments to access student data while parents and children were often denied access.[175] This made it difficult to correct and challenge inaccurate or even stigmatizing information.[176]

FERPA was born in wake of the Watergate scandal and grew out of concerns over government secrecy and the right to access data.[177] Its purpose is to "protect the privacy of student education records."[178] The law applies to all schools that receive any funding that is considered applicable under the U.S. Department of Education.[179] Further, under FERPA, parents and

169 Polonetsky & Tene, *supra* note 157, at 972.

170 20 U.S.C. § 1232h(c)(2)(C)(i) (2012).

171 *See generally*, 20 U.S.C. § 1232h.

172 U.S. DEPARTMENT OF EDUCATION, MODEL NOTIFICATION OF RIGHTS UNDER THE PROTECTION OF PUPIL RIGHTS AMENDMENT (PPRA) (2014), https://www2.ed.gov/policy/gen/guid/fpco/ppra/modelnotification.html.

173 Polonetsky & Tene, *supra* note 157, at 959.

174 Polonetsky & Tene, *supra* note 157, at 959.

175 Polonetsky & Tene, *supra* note 157, at 959.

176 Polonetsky & Tene, *supra* note 157, at 959.

177 Polonetsky & Tene, *supra* note 157, at 959-60.

178 The Family Educational Rights and Privacy Act, 20 U.S.C § 1232g.

179 *Id*.

eligible students (students over the age of eighteen) are granted certain rights in terms of data collection and review.[180] FERPA is meant to promote privacy by preventing schools from needlessly and inappropriately releasing personal data to outside individuals and organizations.[181]

V. AMENDING FERPA AS A MEANS OF MITIGATING FRT HARM

In reviewing these three statutes, the most protection for students in the face of FRT exists under FERPA. Though not a solution to every concern addressed in Part IV of this comment, amendments to FERPA may hold the most potential to mitigate harms. In regard to social concerns, allowing students and parents the ability to review records and challenge disciplinary actions may alleviate negative effects of over-surveillance. Amendments to FERPA may also promote biometric data security.

The NYCLU's letter to Lockport briefly mentions FRT's potential FERPA violations.[182] Commissioner Elia stated, "[s]tudent images are clearly a protected part of a student's biometric record which is included in the definition of 'personally identifiable information' under FERPA."[183] In analyzing the protection of a student's faceprint under FERPA, as the NYCLU suggests, it is also pertinent to interpret the definition of "education records." Under FERPA, student education records are defined as records that: (1) directly relate to a student; and (2) are maintained by an educational agency or institution or by a party acting for the agency or institution.[184] This definition suggests that FERPA only protects those documents affirmatively kept or collected by a school.[185] Additionally, FERPA defines "personally identifiable information" to include direct identifiers and indirect identifiers.[186] Direct identifiers include information such as student's date of birth, place of birth, or mother's maiden name.[187] Indirect identifiers, on the other hand, are a catch-all category of sorts that includes "other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community. . . to identify the student with reasonable certainty."[188]

---

180 *Id*.
181 Polonetsky & Tene, *supra* note 157, at 960.
182 *See* Press Release, *supra* note 11.
183 Curr, *supra* note 8, at 3.
184 20 U.S.C. § 1232g(a)(4)(A) (2012).
185 *Id*.
186 34 C.F.R. § 99.3 (2014) (defining personally identifiable information).
187 *Id*.
188 *Id*.

This definition suggests biometric data should be protected; however, there are several clauses that significantly weaken the statute. Mainly, FERPA authorizes the disclosures of student data without parental consent or opt-out rights in transactions related to the "educational function of the institution;" these transactions include sending information to "school officials," other educational agencies, and federal and state authorities.[189]

The "school officials" element of the 2009 FERPA amendment also includes vendors; thus, so long as vendors are using information for designated educational purposes and act under school control, the transfer of the data is not in violation of FERPA's provisions.[190] This provision is what allows many technology vendors that work with schools to qualify as "school officials."[191] This is worrisome, especially with regards to FRT, as studies have found that commercial companies often fail to impose certain data deletion requirements that are mandated under FERPA.[192]

FERPA has been heavily critiqued for its inability to impose any real sanctions on schools that violate its requirements.[193] Critics of the law have stated that FERPA's sanctions are "so implausible it has never been imposed in the 35-year history of the law. That sanction is a withdrawal of all federal funds. It will never happen."[194] Another one of FERPA's shortcomings is the very fact that "authority" over the data transfers to the child once they turn eighteen.[195] In the past, this provision did not pose a problem as data consisted mostly of areas such as disciplinary actions, a student's transcript, and assessments of the student made by teachers.[196] Now, however, advancements in technology have revolutionized data collection and storage, making data infinitely more sensitive.[197]

Finally, the U.S. Department of Education's Family Policy Compliance Office has yet to offer formal guidance on how to determine if surveillance footage should be subsumed into FERPA. While general video surveillance is not considered an education record, a video showing a student committing acts such as breaking into a locker or getting into a fight will become a

189 Polonetsky & Tene, *supra* note 157, at 963.

190 Polonetsky & Tene, *supra* note 157, at 964.

191 Polonetsky & Tene, *supra* note 157, at 964.

192 Polonetsky & Tene, *supra* note 157, at 954.

193 Polonetsky & Tene, *supra* note 157, at 967.

194 Polonetsky & Tene, *supra* note 157, at 967 (citing Daniel J. Solove, *FERPA and the Cloud: What FERPA Can Learn from HIPPA*, LINKEDIN (Dec. 17, 2012), https://www.linkedin.com/pulse/20121218131535-2259773-ferpa-and-the-cloud-what-ferpa-can-learn-from-hipaa). Daniel J Solove is a Professor of Law at George Washington University Law School, one of the world's leading experts in privacy law, and advocates for FERPA's reform.

195 Polonetsky & Tene, *supra* note 157, at 968.

196 Polonetsky & Tene, *supra* note 157, at 968.

197 Polonetsky & Tene, *supra* note 157, at 969.

demerit if the school uses it for disciplinary purposes.[198] Thus, it is questionable as to whether or not the biometric data collected would even be protected by FERPA unless it was capturing an act of discipline.

In the face of inevitable FRT encroachment, perhaps the best precaution that can be taken is either an amendment to FERPA that specifically includes the use of FRT and biometric data, or the creation and implementation of a new regulation entirely. Additionally, specific protocol should be defined in schools that choose to use FRT. First, it should be made clear to students that the technology will be used solely for the purpose of safety and keeping those that are unwanted out of the building, rather than to monitor each child and punish them for minor offenses. Second, Schools should also be prohibited from sharing the data collected with any and all third-party entities, independently ensure that the data is encrypted, and secure and impose some sort of mandatory data deletion after a certain amount of time has lapsed. Last, schools should be encouraged to employ standards that are commonly promoted when standard surveillance cameras are used.[199] Concepts such as minimizing the amount of areas that host a camera, ensuring transparency and openness about the system, and properly training the staff who will ultimately work the technology would be highly beneficial.[200] Transparency and openness about the system should also be conveyed to students and faculty. If the proper procedures are followed and federal regulations can timely catch up with the technology, FRT may be an effective and vigorous means of safety for modern American schools. [201]

VI. CONCLUSION

The current installation of FRT in the Lockport School District has illuminated a Fourth Amendment right to privacy issue that has been steeping in American public schools for decades. Further, it is clear that through the means of commercial tech-companies, FRT will become more accessible and will be implemented in schools nationwide in time. Though the NYCLU has proposed that the activity come to a full-halt due to the unconstitutionality of the FRT systems, it is unlikely that current jurisprudence or regulatory schemes will offer much protection to students. In order to affirmatively ensure students are protected, it is crucial that the federal government begin to either amend pre-existing Acts such as FERPA or create new ones entirely.

198 Tucker & Vance, *supra* note 54, at 13 (citation omitted).
199 Tucker & Vance, *supra* note 54, at 3.
200 Tucker & Vance, *supra* note 54, at 16.
201 Tucker & Vance, *supra* note 54, at 17.