NORTH CAROLINA LAW REVIEW

Volume 98 | Number 2 Article 12

1-1-2020

School Surveillance: The Students' Rights Implications of Artificial Intelligence as K-12 School Security

Maya Weinstein

School of Surveillance: The Students' Rights Implications of Artificial Intelligence as K-12 Public School Security*

Concerns about school safety dominate the nation as school shootings leave parents, children, and school officials in constant fear. In response to the violence, some schools are acquiring advanced artificial intelligence surveillance technology, including facial recognition and geolocation tracking devices, to strengthen security. The companies behind these technologies claim they will improve school safety. However, there is little indication that they are effective or accurate. Moreover, there is even less information regarding the implications to student privacy and the potential negative impact on the educational environment. Studies prove facial recognition technologies are biased against people of color, which could have devastating effects on students who are already at risk of being pushed out of school through the school-to-prison pipeline. This Comment focuses on public K-12 schools. It includes a review of the efficacy and accuracy of the technologies, analysis of relevant privacy laws, and assessment of the impact on the academic environment. It concludes that the many risks associated with introducing artificial intelligence surveillance technologies into schools must be evaluated through interdisciplinary conversation and should be explored prior to implementation.

INTRODUCTION

The publicity around gun violence in schools has increased since the late 1990s, marked by horrific examples of mass shootings in the halls of K-12 schools and on college campuses.[1] While the exact number of school shootings is disputed,[2] the impact of school violence is undeniable. A national poll

1. *See, e.g.*, James Barron, *Nation Reels After Gunman Massacres 20 Children at School in Connecticut*, N.Y. TIMES (Dec. 14, 2012), https://www.nytimes.com/2012/12/15/nyregion/shooting-reported-at-connecticut-elementary-school.html [https://perma.cc/VZ27-VB7R (dark archive)]; Elizabeth Chuck, Alex Johnson & Corky Siemaszko, *17 Killed in Mass Shooting at High School in Parkland, Florida*, NBC NEWS (Feb. 14, 2018), https://www.nbcnews.com/news/us-news/police-respond-shooting-parkland-florida-high-school-n848101 [https://perma.cc/L7DJ-AVF8]; Christine Hauser & Anahad O'Connor, *Virginia Tech Shooting Leaves 33 Dead*, N.Y. TIMES (Apr. 16, 2007), https://www.nytimes.com/2007/04/16/us/16cnd-shooting.html [https://perma.cc/442T-D34Q (dark archive)]; Brittney Martin et al., *'Overwhelming Grief': 8 Students, 2 Teachers Killed in Texas High School Shooting*, WASH. POST (May 20, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/05/19/ten-killed-in-texas-high-school-shooting-were-mostly-students-police-say-suspect-confessed [https://perma.cc/L4JD-YVBG (dark archive)]; Mark Obmascik, *Columbine High School Shooting Leaves 15 Dead, 28 Hurt*, DENVER POST (Apr. 21, 1999), http://extras.denverpost.com/news/shot0420a.htm [https://perma.cc/K7KJ-TE36].

2. As a result of differing definitions and terminology used in data collection and analysis, the exact number of school shootings in the United States is unclear. *See* Saeed Ahmed & Christina Walker, *There Has Been, on Average, 1 School Shooting Every Week This Year*, CNN (May 25, 2018), https://www.cnn.com/2018/03/02/us/school-shootings-2018-list-trnd/index.html [https://perma.cc/JWS3-EWQB] (including accidental discharge of a firearm). *But see* Chris Wilson, *This Chart Shows the Number of School Shooting Victims Since Sandy Hook*, TIME (Feb. 22, 2018), http://time.com/5168272/how-many-school-shootings/ [https://perma.cc/4VHE-NSUZ (dark archive)] (excluding accidental discharge of a firearm). The United States Department of Education's 2015–16 Civil Rights Data Collection report revealed a number of schools had incidents of gun violence. OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF EDUC., 2015–16 CIVIL RIGHTS DATA COLLECTION SCHOOL CLIMATE AND SAFETY 2 (May 2019), https://www2.ed.gov/about/offices/

conducted in 2018 revealed that one-third of parents now fear for their children's physical safety in school, a statistic that reflects a twenty-two percent increase since 2013.[3] Another survey reported that "[t]wenty percent of parents say their child has expressed concern to them about feeling unsafe at their school."[4] The March For Our Lives movement,[5] started by survivors of the 2018 mass shooting[6] at Marjory Stoneman Douglas High School,[7] saw an estimated 800,000 people turn out for its rally in Washington, D.C., to advocate for gun violence prevention legislation.[8] In 2018 alone, state legislatures considered more than 300 school safety bills and signed over fifty into law.[9]

Student safety has also gained considerable traction as a priority within the federal government. Citing the Marjory Stoneman Douglas shooting as an

list/ocr/docs/school-climate-and-safety.pdf [https://perma.cc/R5JL-QBL3] ("Nearly 230 schools (0.2 percent of all schools) reported at least 1 incident involving a school-related shooting . . . ."). However, the accuracy of the study was called into dispute after schools denied that many of the incidents had occurred and complaints regarding confusing wording in the questionnaire came to light. *See* Anya Kamenetz, Alexis Arnold & Emily Cardinali, *The School Shootings That Weren't*, NPR (Aug. 27, 2018), https://www.npr.org/sections/ed/2018/08/27/640323347/the-school-shootings-that-werent [https://perma.cc/V64L-D2DP] ("NPR reached out to every one of those schools repeatedly over the course of three months and found that more than two-thirds of these reported incidents never happened.").

3. PHI DELTA KAPPAN, THE 50TH ANNUAL PDK POLL OF THE PUBLIC'S ATTITUDES TOWARD THE PUBLIC SCHOOLS K9 (2018), http://pdkpoll.org/assets/downloads/pdkpoll50_2018.pdf [https://perma.cc/KP8Y-XD5U]; *see also* Jeffrey M. Jones, *More Parents, Children Fearful for Safety at School*, GALLUP (Aug. 24, 2018), https://news.gallup.com/poll/241625/parents-children-fearful-safety-school.aspx [https://perma.cc/49FJ-6ZVU] (reporting thirty-five percent of parents "fear for their child's safety at school").

4. Jones, *supra* note 3.

5. MARCH FOR OUR LIVES, https://marchforourlives.com [https://perma.cc/8HJ5-XZ69].

6. The phrase "mass shooting" is not uniformly defined. Emily Alfin Johnson, *What Is a Mass Shooting? Why We Struggle To Agree on How Many There Were This Year*, WAMU (Aug. 4, 2019), https://wamu.org/story/19/08/04/what-is-a-mass-shooting-why-we-struggle-to-agree-on-how-many-there-were-this-year/ [https://perma.cc/MRG8-5E52]; Jason Puckett & David Tregde, *VERIFY: Claims of Over 250 'Mass Shootings' in 2019 Need Context; Could Be Closer to 30*, WUSA9 (Aug. 5, 2019), https://www.wusa9.com/article/news/verify/verify-claims-of-over-250-mass-shootings-in-2019-need-context-could-be-closer-to-30/507-17aae119-8dd5-40f6-b73a-e083324ed795 [https://perma.cc/RRV4-S67K]. For the purposes of this Comment, mass shooting refers to shooting incidents in which four or more people are injured or killed by a gun. *See* Johnson, *supra*; Puckett & Tregde, *supra*.

7. Chuck et al., *supra* note 1.

8. Jessica Durando, *March For Our Lives Could Be the Biggest Single-Day Protest in D.C.'s History*, USA TODAY (Mar. 24, 2018), https://www.usatoday.com/story/news/nation/2018/03/24/march-our-lives-could-become-biggest-single-day-protest-d-c-nations-history/455675002/ [https://perma.cc/3ZXQ-ZAZQ].

9. Alexis Arnold, *Bills and Bulletproof Backpacks: Safety Measures for a New School Year*, NPR (Aug. 16, 2018), https://www.npr.org/2018/08/16/636005341/bills-and-bulletproof-backpacks-safety-measures-for-a-new-school-year [https://perma.cc/C7E7-BJR6]; *see also* Heidi Macdonald & Zeke Perez, *50-State Comparison: K-12 School Safety*, EDUC. COMMISSION STS. (Feb. 25, 2019), https://www.ecs.org/50-state-comparison-k-12-school-safety/ [https://perma.cc/7LP3-PZE7] (discussing state firearm policies for schools); *State Education Policy Tracking*, EDUC. COMMISSION STS. (Feb. 17, 2017), https://www.ecs.org/state-education-policy-tracking/ [https://perma.cc/P94Q-8Z4M].

impetus,[10] President Trump created the U.S. Department of Education's Federal Commission on School Safety[11] in March 2018 to study violence in schools and provide recommendations for proactive measures at the federal, state, and local levels to prevent school violence, mitigate outcomes of violent actions, and facilitate efficient responses to violent situations.[12] The recommendations incorporate "best practices for school building security," including the use of technologies like video surveillance and screening systems.[13]

In response to the fears of additional school violence and calls for enhanced school security, schools have begun tightening security through the use of emerging technologies.[14] While basic security cameras have been used as monitoring devices in schools for years, some schools are looking to more advanced technologies to gain a greater level of control over the campus environment.[15] Recognizing the market opportunity, technology companies are developing new devices they claim will prevent or reduce the likelihood of school shootings.[16] These new devices, which include advanced cameras and

10. *See* FED. COMM'N ON SCH. SAFETY, U.S. DEP'T OF EDUC., FINAL REPORT OF THE FEDERAL COMMISSION ON SCHOOL SAFETY 5 (Dec. 18, 2018) [hereinafter FINAL REPORT], https://www2.ed.gov/documents/school-safety/school-safety-report.pdf [https://perma.cc/9SWU-DWL2].

11. The Federal Commission on School Safety was tasked with "providing meaningful and actionable recommendations to keep students safe at school." *Federal Commission on School Safety*, U.S. DEP'T EDUC., https://www.ed.gov/school-safety [https://perma.cc/SC3E-KZGF]. After months of listening sessions, field visits, and outreach to stakeholders, *id.*, the Commission released its final report in December 2018, *see* FINAL REPORT, *supra* note 10.

12. *See* FINAL REPORT, *supra* note 10, at 126–27 (specifically addressing gun violence and building security improvements for prevention of violence).

13. *Id*. at 119, 122–23.

14. *See, e.g.*, Kaitlyn DeHaven, *Texas ISD Makes Major Security Upgrades Over the Summer*, CAMPUS SECURITY & LIFE SAFETY (Aug. 9, 2019), https://campuslifesecurity.com/articles/2019/08/09/texas-isd-makes-major-security-upgrades-over-the-summer.aspx [https://perma.cc/3YFR-TZ47] ("Two apps will now be used as part of the security measures—the Anonymous Alerts app and the Smart Button. . . . In terms of physical security, the district installed video intercoms at each school entrance."); Mark Keierleber, *Inside the $3 Billion School Security Industry: Companies Marketed Sophisticated Technology To 'Harden' Campuses, but Will It Make Us Safe?*, 74 (Aug. 9, 2018), https://www.the74million.org/article/inside-the-3-billion-school-security-industry-companies-market-sophisticated-technology-to-harden-campuses-but-will-it-make-us-safe/ [https://perma.cc/5JY6-HVBE] ("Schools have increasingly locked and monitored campus entrances in recent years, though the rise in school security is most evident in the growth of video surveillance.").

15. *See* Keierleber, *supra* note 14.

16. The media streaming company RealNetworks is offering its facial recognition software to over 100,000 school districts for free, with the goal of making schools safer. Eli Zimmerman, *Company Offers Free Facial Recognition Software To Boost School Security*, EDTECH (Aug. 3, 2018), https://edtechmagazine.com/k12/article/2018/08/company-offers-free-facial-recognition-software-boost-school-security [https://perma.cc/4V9N-TMSD]; *see also* Press Release, SAFR, RealNetworks Provides SAFR Facial Recognition Solution for Free to Every K-12 School in the U.S. and Canada (July 17, 2018), https://safr.com/press-release/realnetworks-provides-safr-facial-recognition-solution-for-free-to-every-k-12-school-in-the-u-s-and-canada/ [https://perma.cc/W9LZ-TA65] ("School safety

body scanners,[17] use biometrics and artificial intelligence ("AI") to recognize faces; detect weapons, gunshots, and other threats; and track individuals' locations in schools.[18] For the purposes of addressing school security, the main focuses of this Comment are facial recognition, ballistic detection, threat assessment, and location tracking, which schools have begun introducing in recent years.[19]

Despite the purported promise of biometric and AI technologies to protect students, these innovations present troubling students' rights concerns. An inherent tension exists between the desire to protect students from violence through the installation of biometric and AI technologies and the rights students—children—must sacrifice in service of that goal, namely their fundamental right to privacy.[20] These technologies are intrusive; they involve capturing images of children, recording fingerprints, scanning social media, and tracking everything from movements to facial expressions.[21] This is a significant amount of information to be recorded and associated with young people.

has become one of the top national issues in the United States in 2018. . . . We hope this will help make schools safer."); Austin Cushing, *What Should Schools Consider Regarding Metal Detectors and X-Ray Scanners As Security Measures?*, ANCHORTEX CORP. (Sept. 29, 2016), https://www.anchortex.com/company/blog/94-what-should-schools-consider-regarding-metal-detectors-and-x-ray-scanners-as-security-measures [https://perma.cc/D85S-H8PA] ("The National Institute of Justice confirms in its project, The Appropriate and Effective Use of Security Technologies in U.S. Schools, that walk-through metal detectors work well at detecting most types of firearms and knives, and can be used as part of a school environment.").

17. *See* sources cited *supra* note 16.

18. *See infra* Part I.

19. *See infra* Part I. For an analysis of the broader array of school surveillance technologies that makes up the "surveillance state" in North Carolina, see Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. REV. 1673 (2019).

20. The tension between security and privacy in the wake of deadly attacks is no new phenomenon. After the terror attacks on September 11, 2001, office buildings and airports adopted proactive approaches to security to meet the call for risk reduction. *See, e.g.*, Roger Vincent, *Office Building Security Tightened After 9/11*, L.A. TIMES (Sept. 10, 2011), http://articles.latimes.com/2011/sep/10/business/la-fi-911-highrise-security-20110910 [https://perma.cc/GA57-V9RN (dark archive)] (explaining the increase in office building security in major cities); *see also* Jason Villemez, *9/11 to Now: Ways We Have Changed*, PBS NEWS HOUR (Sept. 14, 2011), https://www.pbs.org/newshour/world/911-to-now-ways-we-have-changed [https://perma.cc/MH8B-BFVC] (citing the passage of the Aviation and Transportation Security Act two months after the attacks). These post-9/11 security protocols have raised the contentious question of how to balance individual civil liberties with national security. *See* Kathleen Hicks, *What Will Americans Do About Their Fear of Terrorism?*, ATLANTIC (Aug. 17, 2016), https://www.theatlantic.com/politics/archive/2016/08/the-state-of-national-security-after-911/496046/ [https://perma.cc/6D6Z-RCAW (dark archive)] (indicating, in addition, that "[c]urrent debates over the best way to balance individual rights with security in the context of government surveillance have antecedents in the treatment of anti-war and civil-rights figures during the 1960s and 1970s"); *see also* Sahil Chinoy, *We Built an 'Unbelievable' (but Legal) Facial Recognition Machine*, N.Y. TIMES (Apr. 16, 2019), https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html [https://perma.cc/SE53-KS5B (dark archive)] (discussing facial recognition technology in New York and the lack of state and federal regulation).

21. *See infra* Part I.

Students may not understand the extent to which their personal information is being collected and shared, and high-level surveillance may alter the nature of the educational environment. While schools certainly need to prioritize student safety, the degree to which new surveillance technologies compromise student privacy is alarming.

The threat to student privacy is even more concerning given that these technologies are in their infancy. There is little evidence that they are effective or accurate, and there is even less information regarding the types of risks they pose to students and how to mitigate them.[22] School districts are investing in costly security systems and sharing student data with law enforcement and security companies[23] all in the name of protecting students, but most of these technologies have not been proven to stop school shootings.[24] Some critics have challenged the accuracy of devices, such as facial recognition scanners, particularly when it comes to identification of younger people—the main focus in K-12 schools—and people of color, who already experience surveillance and law enforcement intrusion at disproportionate rates.[25]

22. *See* Stefanie Coyle & John A. Curr III, *Facial Recognition Cameras Do Not Belong in Schools*, NYCLU (June 18, 2018), https://www.nyclu.org/en/news/facial-recognition-cameras-do-not-belong-schools [https://perma.cc/BJZ7-ZJXU] (describing the "potential to turn every step a student takes into evidence of a crime"); Sarah St. Vincent, *Facial Recognition Technology in US Schools Threatens Rights*, HUM. RTS. WATCH (June 21, 2019), https://www.hrw.org/news/2019/06/21/facial-recognition-technology-us-schools-threatens-rights [https://perma.cc/BJZ7-ZJXU] (explaining that facial recognition technology in schools may harm children of color). Additionally, there are added complexities for K-12 schools, as opposed to higher education institutions, because the vast majority of students are minors.

23. *See* Sara Collins, Tyler Park & Amelia Vance, *Ensuring School Safety While Also Protecting Privacy*, FUTURE PRIVACY F. (June 6, 2018), https://fpf.org/2018/06/06/ensuring-school-safety-while-also-protecting-privacy-fpf-testimony-before-the-federal-commission-on-school-safety/ [https://perma.cc/6VE8-BSKJ] ("Schools are using services such as social media monitoring, digital video surveillance linked to law enforcement, and visitor management systems to help protect their students."); Ivan Moreno, *AI-Powered Cameras Become New Tool Against Mass Shootings*, ASSOCIATED PRESS (Aug. 30, 2019), https://www.apnews.com/eca5dcff514b49eb8edaaf301d0a3a3d [https://perma.cc/7NMG-Q79J]. Lockport City School District in New York faced backlash from parents and the New York Civil Liberties Union after investing $3.3 million in a facial recognition system. *See* Thomas J. Prohaska, *Lockport Schools Turn to State-of-the-Art Technology To Beef Up Security*, BUFFALO NEWS (May 20, 2018) [hereinafter Prohaska, *Beef Up Security*], https://buffalonews.com/2018/05/20/lockport-schools-turn-to-state-of-the-art-technology-to-beef-up-security/ [https://perma.cc/5T6L-ZGV6 (dark archive)]; Thomas J. Prohaska, *NYCLU Attacks Lockport Schools' Facial Recognition Security Plan*, BUFFALO NEWS (Sept. 3, 2018), https://buffalonews.com/2018/09/03/nyclu-attacks-lockport-schools-facial-recognition-security-plan/ [https://perma.cc/5T6L-ZGV6 (dark archive)].

24. *See* Drew Harwell, *Unproven Facial-Recognition Companies Target Schools, Promising an End to Shootings*, WASH. POST (June 7, 2018), https://www.washingtonpost.com/business/economy/unproven-facial-recognition-companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637_story.html [https://perma.cc/7DKL-5UJA (dark archive)].

25. *See* Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016), https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html [https://perma.cc/DA3W-LNM8] (describing the National Security

This Comment addresses key legal issues surrounding advanced security technologies in public K-12 schools, including the impact on student privacy rights under relevant laws. It also explores the effects these technologies have on the educational environment. It argues that, in using AI surveillance technology in schools, privacy must be balanced against security concerns; the apparent issues with efficacy and accuracy of the technology should be addressed before implementation; and Fourth Amendment case law, federal student privacy legislation, and state laws need to be further developed, with states leading the way, to ensure the protection of students' rights. The scope of the analysis is limited to public schools because these schools are subject to more government control than private schools.[26]

Part I presents background on AI technologies and an overview of the technologies that are currently in use or are in development for school surveillance. Part II addresses potential harms to students resulting from AI surveillance in schools, including the implications of accuracy and efficacy issues in AI algorithms. Part III delves into the application of relevant privacy laws, specifically the Fourth Amendment, the Family Educational Rights and Privacy Act ("FERPA"), and state laws, and demonstrates that the law has not progressed to the point of effectively protecting students from AI surveillance. In the end, this Comment argues that schools and governments have more work to do to protect students from technological intrusions that undermine their basic rights.

I. OVERVIEW OF ADVANCED TECHNOLOGIES

Gone are the days when school security simply meant a parent volunteer at the front office, student IDs with outdated photos, or low-quality cameras that produced grainy images from afar. Today's surveillance options are in a constant state of technological development, utilizing advanced methods that resemble Orwell's predictions.[27] This part begins with an overview of the

Association's wiretapping of Martin Luther King Jr., surveillance of Japanese Americans during World War II, and the monitoring of shops in majority-Muslim neighborhoods post-September 11, 2001).

26. *See The Federal Role in Education*, U.S. DEP'T EDUC., https://www2.ed.gov/about/overview/fed/role.html [https://perma.cc/4C8V-RE69]; Stephanie Watson, *How Public Schools Work*, HOW STUFF WORKS, https://people.howstuffworks.com/public-schools2.htm [https://perma.cc/AM5P-MYVE]. In comparison to public schools, private schools are subject to less regulation. *See generally* U.S. DEP'T OF EDUC., STATE REGULATION OF PRIVATE SCHOOLS (2009) [hereinafter STATE REGULATION OF PRIVATE SCHOOLS], https://www2.ed.gov/admins/comm/choice/regprivschl/regprivschl.pdf [https://perma.cc/7FGW-R3UG] (illustrating the minimal regulatory requirements for private schools).

27. *See, e.g.*, Patrick Law Grp., LLC, *When 2017 Becomes 1984: Facial Recognition Technologies—Face a Growing Legal Landscape*, JD SUPRA (Oct. 5, 2017), https://www.jdsupra.com/legalnews/when-2017-becomes-1984-facial-79060/ [https://perma.cc/H82U-C6JQ]. Despite some parallels between Orwell's predictions and current technology, most of the surveillance systems depicted in the classic dystopian novel *1984* were far more advanced than what is being used in the United States today—as

mechanics of biometric and AI technology. It then describes the specific types of technologies in use for security in schools.

Biometric technology is "the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for purposes of recognizing that individual."[28] Biometrics may include "fingerprints, DNA, facial recognition, iris and retina scans, vein structure, walking gait, and voice recognition."[29] For example, when an individual uses her thumbprint to unlock a cellphone, biometric technology is used to recognize her specific thumbprint and unlock the phone.

Artificial intelligence takes biometric data to the next level. AI involves machines or technologies completing tasks we typically think of as being performed by humans.[30] There is no single accepted definition of AI,[31] but it can be defined through categorizations of what it does or how it works: AI engages in perception, natural language processing, logical reasoning, planning and navigation, and knowledge representation.[32] While there are multiple subfields of AI, "machine learning" has garnered a significant amount of attention.[33] Machine learning is "a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with

far as we know. Rob Beschizza, *Does the Technology of Orwell's 1984 Really Exist?*, WIRED (Feb. 5, 2008), https://www.wired.com/2008/02/does-the-techno/ [https://perma.cc/WW9E-75V9 (dark archive)].

28. John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 99 (1997).

29. Robee Krishan & Reza Mostafavi, *Biometric Technology: Security and Privacy Concerns*, J. INTERNET L., July 2018, at 19, 19.

30. Janna Anderson & Lee Rainie, *Artificial Intelligence and the Future of Humans*, PEW RES. CTR. (Dec. 10, 2018), https://www.pewinternet.org/2018/12/10/artificial-intelligence-and-the-future-of-humans/ [https://perma.cc/VN2F-Q8JB].

31. Matt Chessen, *What Is Artificial Intelligence? Definitions for Policy-Makers and Non-Technical Enthusiasts*, MEDIUM (Apr. 3, 2017), https://medium.com/artificial-intelligence-policy-laws-and-ethics/what-is-artificial-intelligence-definitions-for-policy-makers-and-laymen-826fd3e9da3b [https://perma.cc/LG29-S69H]. AI may be defined broadly as "a computerized system that exhibits behavior that is commonly thought of as requiring intelligence" or as "a system capable of rationally solving complex problems or taking appropriate actions to achieve its goals in whatever real world circumstances it encounters." NAT'L SCI. & TECH. COUNCIL, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE 6 (2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf [https://perma.cc/YD9L-6G56].

32. Frank Chen, *AI, Deep Learning, and Machine Learning: A Primer*, ANDREESSEN HOROWITZ (June 10, 2016), https://a16z.com/2016/06/10/ai-deep-learning-machines/ [https://perma.cc/35AT-FL9S].

33. *See, e.g.*, Louis Columbus, *State of AI and Machine Learning in 2019*, FORBES (Sept. 8, 2019), https://www.forbes.com/sites/louiscolumbus/2019/09/08/state-of-ai-and-machine-learning-in-2019/#7259621a1a8d [https://perma.cc/92VF-BTB2]; Ingrid Fidelli, *Using Machine Learning To Reconstruct Deteriorated Van Gogh Drawings*, TECH XPLORE (Sept. 20, 2019), https://techxplore.com/news/2019-09-machine-reconstruct-deteriorated-van-gogh.html [https://perma.cc/9FWT-UBJJ].

minimal human intervention."[34] Through a system of algorithms, machine learning "enables computers to learn from experience or examples."[35]

When AI is paired with biometrics, like facial recognition cameras or fingerprint scanners, the technologies are able to more deeply assess the content they are exploring.[36] Instead of simply capturing a photographic image or copying a thumbprint, the system can run the information through a database, look for a match, and then take action, like automatically opening a door.[37] In the context of security, some companies are embedding their technologies with machine learning and biometrics so that, for example, "the system is taught to identify an object as a threat based on certain characteristics—such as the signature [features] of a gun, knife or bomb."[38] A system is trained by being fed numerous images and asked to identify them until the system improves—or "learns"—to the point where it identifies images at a high level of accuracy and precision.[39]

In schools, biometric and AI technologies cover a wide spectrum of programs. The AI industry has seen a massive boom within the education market, and the worldwide AI education market value is predicted to surpass six billion dollars by 2024,[40] with classroom applications accounting for twenty percent of that growth.[41] Much of the reason for this growth is the integration

34. *Machine Learning: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/analytics/machine-learning.html [https://perma.cc/NVJ3-W8QQ].

35. NAT'L SCI. & TECH. COUNCIL, THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH & DEVELOPMENT STRATEGIC PLAN 5 (2016), https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf [https://perma.cc/F75U-43SY]. Deep learning, a more complex branch of AI, has also made waves. *See id*. at 5 n.4 (describing deep learning as "a general family of methods that use multi-layered neural networks").

36. Naveen Joshi, *Biometrics Is Smart, but AI Is Smarter. Here's Why*, ALLERIN (Apr. 9, 2019), https://www.allerin.com/blog/biometrics-is-smart-but-ai-is-smarter-heres-why [https://perma.cc/RN7S-LVKK] ("AI and biometrics can work together to develop effective and reliable security models.").

37. *See, e.g.*, Stanley Goodner, *Finger Scanners: What They Are and Why They Are Gaining in Popularity*, LIFEWIRE (June 24, 2019), https://www.lifewire.com/understanding-finger-scanners-4150464 [https://perma.cc/7R9X-L2MB]; Ronnie Wendt, *Facial Recognition Technology Faces Scrutiny*, SECURITY SALES & INTEGRATION (July 30, 2019), https://www.securitysales.com/news/facial-recognition-tech-scrutiny/ [https://perma.cc/FK7H-HTUM].

38. Jennifer Kite-Powell, *Making Facial Recognition Smarter with Artificial Intelligence*, FORBES (Sept. 30, 2018), https://www.forbes.com/sites/jenniferhicks/2018/09/30/making-facial-recognition-smarter-with-artificial-intelligence/#2611c94cc8f1 [https://perma.cc/GE69-XUQ6].

39. *See* Danny Sullivan, *How Machine Learning Works, as Explained by Google*, MARTECH TODAY (Nov. 4, 2015), https://martechtoday.com/how-machine-learning-works-150366 [https://perma.cc/UZQ4-DKXV]; *What Is Machine Learning?*, MATHWORKS, https://www.mathworks.com/discovery/machine-learning.html [https://perma.cc/6QB2-9UZ4].

40. Ankita Bhutani & Preeti Wadhwani, *Artificial Intelligence (AI) in Education Market Size Worth $6bn by 2024*, GLOBAL MKT. INSIGHTS (Aug. 12, 2019), https://www.gminsights.com/pressrelease/artificial-intelligence-ai-in-education-market [https://perma.cc/W3RP-SNDQ].

41. Michele Molnar, *K-12 Artificial Intelligence Market Set To Explode in U.S. and Worldwide by 2024*, EDWEEK MKT. BRIEF (July 10, 2018), https://marketbrief.edweek.org/marketplace-k-12/k-12-

of AI systems for personalized learning, which enables students to receive "immediate and personalized feedback and instructions . . . without the intervention of a human tutor."[42] Biometrics have been incorporated into the classroom as well,[43] and some schools even use biometrics to allow students to pay for lunch with just a fingerprint.[44]

Schools are also starting to incorporate AI and biometrics into surveillance programs. One popular new area of school surveillance technology is location tracking. For instance, the program "e-hallpass" is a modern, electronic hall pass that "continuously logs and monitors student time in the halls" and claims to "improv[e] school security and emergency management while reducing classroom disruptions by as much as 50%."[45] A similar program, "iClicker Reef," tracks attendance through a geolocation feature.[46] Using geolocation,[47] these

artificial-intelligence-market-set-explode-u-s-worldwide-2024/ [https://perma.cc/6HBQ-JCEF]; *see* Karen Hao, *China Has Started a Grand Experiment in AI Education. It Could Reshape How the World Learns.*, MIT TECH. REV. (Aug. 2, 2019), https://www.technologyreview.com/s/614057/china-squirrel-has-started-a-grand-experiment-in-ai-education-it-could-reshape-how-the/ [https://perma.cc/4XB4-TBA9 (dark archive)] (describing the development and efficacy of an AI learning center in China).

42. *Artificial Intelligence in Education Market To Hit $6bn by 2024*, GLOBAL MKT. INSIGHTS (June 6, 2018), https://www.globenewswire.com/news-release/2018/06/06/1517441/0/en/Artificial-Intelligence-in-Education-Market-to-hit-6bn-by-2024-Global-Market-Insights-Inc.html [https://perma.cc/C99D-YETS].

43. *E.g.*, Stephanie Babych, *Virtual Reality Project at Lethbridge College Could Change the Way Justice Studies Taught*, CALGARY HERALD (Aug. 31, 2019), https://calgaryherald.com/news/local-news/virtual-reality-project-at-lethbridge-college-could-change-the-way-justice-studies-taught [https://perma.cc/LW5M-HCGM] (describing a program that simulates scenarios police officers may encounter and uses biometrics to test the efficacy of the training); Jen A. Miller, *Biometrics in Schools To Yield Security Benefits and Privacy Concerns*, EDTECH MAG. (May 7, 2019), https://edtechmagazine.com/k12/article/2019/05/biometrics-schools-yield-security-benefits-and-privacy-concerns [https://perma.cc/43XZ-D23B] ("Biometric technology is already part of the K-12 ecosystem, where administrators are using iris scans and 'facial fingerprints' to grant access to buildings and computer labs, track attendance, manage lunch payments, loan library materials and ensure students get on the right buses."); Mae Rice, *13 EdTech Applications that Are Transforming Teaching and Learning*, BUILT IN (June 22, 2019), https://builtin.com/edtech/technology-in-classroom-applications [https://perma.cc/J265-VLXM] (describing an online test proctoring system which confirms test-takers' identities through fingerprints and voice biometrics).

44. *Biometrics Allows Students To Purchase with Fingerprint*, GOV'T TECH. (Oct. 17, 2007), https://www.govtech.com/health/Biometrics-Allows-Students-to-Purchase-with.html [https://perma.cc/E8BS-6QJH].

45. *E-Hallpass*, EDUSPIRE SOLUTIONS, https://www.eduspiresolutions.org/what-is-e-hallpass/ [https://perma.cc/7BBP-TY6L].

46. David Rosen & Aaron Santesso, *How Students Learned To Stop Worrying—and Love Being Spied On*, CHRON. HIGHER EDUC. (Sept. 23, 2018), https://www.chronicle.com/article/How-Students-Learned-to-Stop/244596 [https://perma.cc/XZW2-YKY8 (dark archive)].

47. Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy*, ITWORLD (Mar. 31, 2010), https://www.itworld.com/article/2756095/networking-hardware/geolocation-101--how-it-works--the-apps--and-your-privacy.html [https://perma.cc/AMB3-8VLK] ("Typically, geolocation apps do two things: They report your location to other users, and they associate real-world locations (such as restaurants and events) to your location.").

location systems have the ability to identify when a student is in class, log attendance for the teacher, and track where students are in school.[48]

Facial recognition is another growing category of biometric and AI technology that schools are beginning to use. For example, one private high school implemented a facial recognition[49] camera program that automatically unlocks doors upon recognition of individuals—staff, students, and volunteers—whose photographs have been uploaded into the system database.[50] The school can also upload images of "key undesirables," such as sex offenders or disgruntled employees, and the system will notify administrators if those individuals are seen by the cameras.[51]

Another type of facial recognition program, called "affect recognition," uses biometric analysis to scan individuals' faces and identify emotions.[52] For instance, an Australian university is currently testing a product called the "Biometric Mirror," which reads faces and ranks them according to fourteen characteristics, including gender, age, ethnicity, attractiveness, "weirdness," and emotional stability.[53] Schools in China have implemented a similar technology to analyze students' facial expressions, including expressions like "neutral, happy, sad, disappointed, angry, scared and surprised."[54] The main goal of this

48. Rosen & Santesso, *supra* note 46. Some schools are extending their monitoring programs off campus by scanning students' social media accounts for potential threats. *See* Aleshia Howell, Opinion, *Surveillance Tech Compromises Trust, Safety in Schools*, SAVANNAH NOW (Sept. 19, 2019), https://www.savannahnow.com/opinion/20190919/aleshia-howell-column-surveillance-tech-compromises-trust-safety-in-schools [https://perma.cc/X4XZ-MZ3R].

49. *See Facial Recognition*, TECHOPEDIA, https://www.techopedia.com/definition/32071/facial-recognition [https://perma.cc/AMB3-8VLK] ("Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours.").

50. Peter B. Counter, *Facial Recognition Deployed at St. Louis High School*, FIND BIOMETRICS (Mar. 9, 2015), https://findbiometrics.com/facial-recognition-deployed-at-st-louis-high-school-23094/ [https://perma.cc/G9UM-FLLN]. Although the school in this case is a private school, this Comment does not address private schools beyond this example because they are not subject to the same laws as public schools. STATE REGULATION OF PRIVATE SCHOOLS, *supra* note 26 (providing descriptions of each state's requirements for private schools); *How Are the Local, State and Federal Governments Involved in Education? Is This Involvement Just?*, CTR. FOR PUB. JUST., https://www.cpjustice.org/public/page/content/cie_faq_levels_of_government [https://perma.cc/EB7K-A378] ("Independent schools, which are established by associations, parents or individuals, operate independent of direct government control.").

51. Counter, *supra* note 50.

52. MEREDITH WHITTAKER ET AL., AI NOW REPORT 2018, at 4 (Dec. 2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf [https://perma.cc/2EAJ-AALT] ("Affect recognition is a subclass of facial recognition that claims to detect things such as personality, inner feelings, mental health, and 'worker engagement' based on images or video of faces.").

53. Jo Lauder, *Mirror, Mirror: How AI Is Using Facial Recognition To Decipher Your Personality*, ABC AUSTL. (July 23, 2018), https://www.abc.net.au/triplej/programs/hack/how-ai-is-using-facial-recognition-to-decipher-your-personality/10025634 [https://perma.cc/9VGY-5L5X].

54. Neil Connor, *Chinese School Uses Facial Recognition To Monitor Student Attention in Class*, TELEGRAPH (May 17, 2018), https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/ [https://perma.cc/TM3G-4RHP (dark archive)].

so-called "smart eye" is to alert teachers when students are distracted in class.[55] However, the identification of changes in mood may also assist educators with identifying students experiencing mental health crises, which could help flag potential threats.[56]

The use of technology to analyze student behavior extends beyond the physical classroom. Some schools are already monitoring their students online, using Safety Management Platforms as threat assessment measures to scan school computers for indicators of violence by analyzing the words students type.[57] Threat assessment programs aim to "evaluate the risk posed by a student or another person, typically as a response to an actual or perceived threat or concerning behavior."[58]

A final type of surveillance technology receiving significant attention is ballistic detection. For example, one company's "gunshot defense system" uses artificial intelligence to detect gunshots, alert law enforcement, and engage with the shooter by "delivering intense, non-lethal sound waves and light beams that virtually stops an attacker on the spot, which also creates a diversion to assist students and faculty with additional time to run and hide or escape."[59] Cameras around the building track the shooter's location and deliver updates to law enforcement while the system uses AI to direct victims to the safest exits.[60] The program's developer markets the technology with a video stating that "[t]he majority of the deaths and casualties [in a mass shooting] happen within the first 5 minutes or 300 seconds,"[61] making it imperative to identify and stop a shooter quickly. This type of technology is extremely appealing as it acts as a first line of defense and assists responding law enforcement officers. Other

55. *Id*.

56. *See, e.g.*, Randy Rieland, *Can Artificial Intelligence Help Stop School Shootings?*, SMITHSONIAN (June 22, 2018), https://www.smithsonianmag.com/innovation/can-artificial-intelligence-help-stop-school-shootings-180969288/ [https://perma.cc/7VRZ-2T6Y] (describing the use of machine learning to analyze student language and behavior and help counselors with risk assessment).

57. Simone Stolzoff, *Schools Are Using AI To Track What Students Write on Their Computers*, QUARTZ (Aug. 19, 2018), https://qz.com/1318758/schools-are-using-ai-to-track-what-students-write-on-their-computers/ [https://perma.cc/X9B2-LEHB].

58. *Threat Assessment*, OFF. SUPERINTENDENT PUB. INSTRUCTION, https://www.k12.wa.us/student-success/health-safety/school-safety-center/z-index/threat-assessment [https://perma.cc/VF6E-CTL5]; *see also Threat Assessment for School Administrators & Crisis Teams*, NAT'L ASS'N SCH. PSYCHOLOGISTS, https://www.nasponline.org/resources-and-publications/resources-and-podcasts/school-climate-safety-and-crisis/systems-level-prevention/threat-assessment-at-school/threat-assessment-for-school-administrators-and-crisis-teams [https://perma.cc/KVV7-GMNY] ("The goals of threat assessment are to keep schools safe and to help potential offenders overcome the underlying sources of their anger, hopelessness, or despair.").

59. *300 Seconds Video—School Security Solutions*, SECURITY ORACLE, https://www.thesecurityoracle.com/system-products/school-security-solution [https://perma.cc/4R8G-5LW9].

60. *Id.*

61. *Id.*

companies that use ballistic detection, but different methods of response, have also entered the K-12 market.[62]

Although the technology may sound positive from a security standpoint, these technologies are intrusive and create an environment where students are tracked, monitored, and watched. Many of these programs involve constant monitoring of children, and some collect personally identifying data, including fingerprints and face images. As will be discussed in Parts II and III, there are a number of potential adverse consequences of these technologies: students may be less likely to speak openly in class, risks of false data matches may lead to wrongful disciplinary actions, and the technologies encroach on student privacy rights.

II. EFFICACY AND ACCURACY PROBLEMS WITH AI SURVEILLANCE TECHNOLOGIES

The use of AI surveillance technologies in schools has the potential to alter the academic environment, in large part because the unknown inner workings of the technologies result in problems with accuracy and efficacy. This part addresses the impact of surveillance on students' freedom in the educational setting, which is compounded by the lack of transparency of AI technology developers. The lack of transparency makes it difficult to fully predict the extent of potential issues with the technologies, such as bias in the algorithms that could result in harm to students and their parents. Instead of providing a safer environment, these developments come at the expense of safety, especially given that the efficacy of the technologies in preventing school violence has not been proven.

A. *Impact on the Academic Environment*

One example of the impact new surveillance technologies may have on students comes in the classroom setting. Students who know they are being monitored may not express controversial views, thus suppressing the quality of the academic environment. Students may also avoid sharing personal details out of fear of disciplinary response by their school. While companies claim their surveillance programs are effective in preventing violence, they may also normalize a surveillance state or "have a chilling effect on students' freedom of expression."[63]

62. *See, e.g.*, *EAGL Gunshot Detection & Lockdown System*, EAGL, https://www.eagltechnology.com/eagl-gunshot-detection-lockdown-system/ [https://perma.cc/DY3W-MYF9]; *Firefly & Dragonfly*, EAGL, https://www.eagltechnology.com/firefly-dragonfly/ [https://perma.cc/EZ4M-YBLQ]; *LightAway*, VS ENERGY, https://www.vsenergy.us/lightaway-dynamic-lighting-wayfinding-372034.html [https://perma.cc/BY77-EBLN].

63. Stolzoff, *supra* note 57.

In the higher education setting, there is some evidence that students are willing to withstand surveillance in exchange for efficiency.[64] This is perhaps an even stronger example of the negative impact surveillance at an early age can create. As students of younger generations have little choice in whether to give up information to technology at a young age in K-12 schools, it is not surprising that as they enter adulthood they will think less of the consequences and more of the benefits.

B. *Lack of Transparency and Understanding*

Beyond the impact on the academic environment, the new technology also lacks transparency. Engineers may use AI to train a system to accurately identify, for example, a picture of a turtle, but even the engineers may not know *how* the system reaches its conclusion because the technology is so complex. This "black box"—"the idea that we can understand what goes in and what comes out, but don't understand what goes on inside"—dramatically reduces transparency.[65] While it may not be as concerning in a low-stakes situation that lends itself to easy independent verifiability (like the turtle identification example), misidentification, privacy intrusion, and harms to the educational environment are risks of black box AI that will become more evident should humans rely on machines for critical decisionmaking that impacts people's lives and abilities to achieve an education.[66] Further, AI involves proprietary technologies, meaning companies can protect the inner workings of the machines as intellectual property.[67] This allows companies to maintain secrecy around the programs, so even if the engineers do know how a program is reaching a conclusion, the company does not have to reveal that information. The extent to which information is available regarding the inner workings of AI

64. Rosen & Santesso, *supra* note 46.

65. Tim Sandle, *Crypto, AI and Machine Learning To Shape Enterprises*, DIGITAL J. (Jan. 9, 2019), http://www.digitaljournal.com/print/article/540595 [https://perma.cc/7KRD-HENR].

66. Some courts have begun using AI for recidivist risk assessment without a full understanding of which factors the machines consider, thus raising due process concerns. *See* Noel L. Hillman, *The Use of Artificial Intelligence in Gauging the Risk of Recidivism*, JUDGES' J. 36, 36–38 (2019); Katherine Freeman, Recent Development, *Algorithmic Injustice: How the Wisconsin Supreme Court Failed To Protect Due Process Rights in* State v. Loomis, 18 N.C. J.L. & TECH. 75, 75, 104 (2016); Ed Yong, *A Popular Algorithm Is No Better at Predicting Crimes than Random People*, ATLANTIC (Jan. 17, 2018), https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/ [https://perma.cc/3Q3Y-2ZV2 (dark archive)]. Similar models employed for credit scoring have received criticism for efficacy problems. *See* Rachel O'Dwyer, *Algorithms Are Making the Same Mistakes Assessing Credit Scores that Humans Did a Century Ago*, QUARTZ (May 14, 2018), https://qz.com/1276781/algorithms-are-making-the-same-mistakes-assessing-credit-scores-that-humans-did-a-century-ago/ [https://perma.cc/8NSQ-9VXU].

67. *See* Jessica M. Meyers, *Artificial Intelligence and Trade Secrets*, A.B.A. (Feb. 19, 2019), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/january-february/artificial-intelligence-trade-secrets-webinar [https://perma.cc/8YL5-MXGX].

technologies thus heavily relies on companies' willingness to voluntarily share data, which many companies are hesitant to do.[68]

C. *Efficacy of AI Surveillance To Prevent or Stop School Shootings*

The lofty promises of AI surveillance companies remain unverified; it is not yet certain that these technologies are effective in preventing school shootings. For example, while facial recognition companies are marketing their products as resources to stop prohibited people from entering campus, most school shootings have been committed by students who were permitted to be on campus.[69] Thus, while the technology may work well in a vacuum,[70] the application to the types of shootings that occur at K-12 schools lacks indications of efficacy.[71]

So far, AI has not been proven to be foolproof in even its most basic applications, showing that ill-intentioned people could circumvent AI surveillance technologies in order to access schools. In fact, AI is even capable of tricking AI.[72] In test settings, biometric security systems have been threatened by AI manipulation.[73] In one study, researchers used neural networks to create fake fingerprints in an attempt to fool fingerprint-scanning systems—and it worked.[74] When the fakes tricked the system, it allowed the researchers to refine their technology to create even more realistic and effective fake prints.[75]

68. The National Institute for Standards and Technology offers evaluations of facial recognition programs, but the program is voluntary and there is no oversight or enforcement mechanism. Christina Couch, *Ghosts in the Machine*, PBS: NOVA (Oct. 25, 2017), https://www.pbs.org/wgbh/nova/article/ai-bias/ [https://perma.cc/4CU8-P8W5].

69. Harwell, *supra* note 24. Since 1970, there have been 1300 school shootings. *The K-12 Shooting Statistics Everyone Should Know* (Oct. 15, 2018), https://www.campussafetymagazine.com/safety/k-12-school-shooting-statistics-everyone-should-know/ [https://perma.cc/8NST-5ER6]. Of those, 691 were committed by a current student, while fifty-eight were committed by former students. *Id.*

70. The less risk involved, and the fewer people entered into the database, the more effective the technology. *Face Recognition*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/face-recognition [https://perma.cc/Q6NS-9ASH].

71. Harwell, *supra* note 24 (quoting Andrew Ferguson, a law professor at the University of the District of Columbia, as saying that "[t]hese companies are taking advantage of the genuine fear and almost impotence of parents who want to protect their kids . . . and they're selling them surveillance technology at a cost that will do very little to protect them").

72. Researchers used an AI algorithm to trick Google's image recognition software into identifying a turtle as a rifle "because it identified hidden elements embedded in the image that shared certain properties with an image of a gun, all of which were unnoticeable by the human eye." Jonathan Vanian, *Artificial Intelligence Is Giving Rise to Fake Fingerprints. Here's Why You Should Be Worried*, FORTUNE (Nov. 28, 2018), http://fortune.com/2018/11/28/artificial-intelligence-fingerprints-security/ [https://perma.cc/DL4T-FRAJ].

73. *Id.*

74. *Id.*

75. *Id.*

Fortunately, it takes significant knowledge of the technology to beat it, and many fingerprint sensor software companies employ additional security measures, like heat sensors, to deter attacks.[76] Nonetheless, the fact that AI systems can be tricked shows that these technologies must undergo significant development before they can compete with humans for even some of the most basic uses and certainly before these programs are released for high-level security in schools. Humans must work alongside machines to make final judgment calls and to catch threats that machines fail to identify.[77]

D. *Machine Bias*

A major concern related to implementing AI technologies is the risk of machine bias, which refers to systematic disparities in accuracies of algorithm results, typically with respect to race, but also gender or age.[78] The identification abilities of AI in biometrics are only as good as the humans who develop them. A prominent AI expert and co-founder of AI4ALL[79] described the issue as such: "bias in, bias out."[80]

There is a severe lack of diversity in the artificial intelligence field.[81] One major study found that women make up less than twenty percent of AI professors, conference authors, and research staff at major technology

76. *Id.*

77. *See, e.g.*, James Vincent, *Google's AI Thinks This Turtle Looks Like a Gun, Which Is a Problem*, VERGE (Nov. 2, 2017), https://www.theverge.com/2017/11/2/16597276/google-ai-image-attacks-adversarial-turtle-rifle-3d-printed [https://perma.cc/Z6ML-MCMR].

78. *See* Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/C8DL-NKTU]; *Machine Bias*, TECHOPEDIA, https://www.techopedia.com/definition/33036/machine-bias [https://perma.cc/QQ4R-6BNC]; Margaret Rouse, *Machine Learning Bias (Algorithm Bias or AI Bias)*, SEARCH ENTERPRISE AI, https://searchenterpriseai.techtarget.com/definition/machine-learning-bias-algorithm-bias-or-AI-bias [https://perma.cc/9WB7-K3NF].

79. AI4ALL is a nonprofit "dedicated to increasing diversity and inclusion in AI education, research, development, and policy." *Our Story*, AI4ALL, http://ai-4-all.org/about/our-story/ [https://perma.cc/4JYX-V3UH].

80. Jessi Hempel, *Fei-Fei Li's Quest To Make AI Better for Humanity*, WIRED (Nov. 13, 2018), https://www.wired.com/story/fei-fei-li-artificial-intelligence-humanity/ [https://perma.cc/8ZZM-C95W (dark archive)].

81. *See* SARAH MYERS WEST, MEREDITH WHITTAKER & KATE CRAWFORD, AI NOW INST., DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI *passim* (Apr. 2019), https://ainowinstitute.org/discriminatingsystems.pdf [https://perma.cc/DH8Y-AE94] (highlighting the male domination and lack of people of color in the AI research and development field); *see also* Kari Paul, *'Disastrous' Lack of Diversity in AI Industry Perpetuates Bias, Study Finds*, GUARDIAN (Apr. 16, 2019), https://www.theguardian.com/technology/2019/apr/16/artificial-intelligence-lack-diversity-new-york-university-study [https://perma.cc/L8WT-KEG8]; Jonathan Vanian, *Eye on A.I.—How To Fix Artificial Intelligence's Diversity Crisis*, FORTUNE (Apr. 23, 2019), https://fortune.com/2019/04/23/artificial-intelligence-diversity-crisis/ [https://perma.cc/84AE-9NHD].

companies,[82] and people of color account for less than ten percent of AI engineers at top companies.[83] The demographic makeup of employees of these companies is reflected in the output of the machines.[84] Resulting machine bias is, perhaps, reflective of the cultural perceptions and identities of the engineers. However, it is difficult to study the potential consequences of machine bias when the inner workings of surveillance technologies remain concealed.[85] There is a void in the law when it comes to protecting students against these bias errors. This must be addressed before releasing these largely untested technologies on students.

1. Machine Bias Generally

There is limited research on the accuracy of facial recognition algorithms,[86] and the information that does exist indicates disproportionate misidentification of Black people, women, and young people.[87] False matches, or misidentifications, occur when the system matches a scanned face to the wrong person in a database.[88] For example, individual *X* may be scanned and matched with the profile of fugitive *Y*. Individual *X* is then arrested under the assumption he or she is actually fugitive *Y*.

82. *See* WEST ET AL., *supra* note 81, at 10–11 (finding women constitute eighteen percent of authors at AI conferences in the field, less than twenty percent of AI professors, and between ten and fifteen percent of AI research staff at large tech firms like Facebook and Google).

83. *See id.* at 11 (citing statistics from Google, Facebook, and Microsoft for Black and Latinx employees).

84. *See infra* Section II.D.1; *see also* Angela Benton, *An AI-Run World Needs To Better Reflect People of Color*, WIRED (Sept. 6, 2019), https://www.wired.com/story/an-ai-run-world-needs-to-better-reflect-people-of-color/ [https://perma.cc/YP4G-EZCD (dark archive)] (recommending that incorporating more women and people of color into developer teams will improve potential machine learning algorithms).

85. *See supra* Section II.B.

86. One reason for the lack of research is that these programs are mostly used by law enforcement and such agencies actively try to keep the inner workings obscure. *See* Clare Garvie & Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/ [https://perma.cc/X6X2-RRZF (dark archive)]; Karen Hao, *Police Across the U.S. Are Training Crime-Predicting AIs on Falsified Data*, MIT TECH. REV. (Feb. 13, 2019), https://www.technologyreview.com/s/612957/predictive-policing-algorithms-ai-crime-dirty-data/ [https://perma.cc/ZS9X-KCP3 (dark archive)]. Additionally, law enforcement systems "are not required to undergo public or independent testing," and agencies certainly are not volunteering this information for evaluation. Garvie & Frankle, *supra*.

87. *See, e.g.*, Angwin et al., *supra* note 78 (discussing AI racial bias); Couch, *supra* note 68 (stating that three facial recognition algorithms were less accurate when reading the faces of women, Black people, and younger people); Garvie & Frankle, *supra* note 86 (discussing AI racial bias).

88. *See, e.g.*, Kate Queram, *Face-Recognition Tool Misidentified Lawmakers as Criminals: ACLU*, DEF. ONE (Aug. 17, 2019), https://www.defenseone.com/technology/2019/08/face-recognition-tool-misidentified-state-lawmakers-criminals-aclu/159190/ [https://perma.cc/8CJ9-F8E6]; Tom Simonite, *The Best Algorithms Struggle To Recognize Black Faces Equally*, WIRED (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [https://perma.cc/7H8S-J45R (dark archive)].

Misidentification is likely caused by problems with the development and training of the software. A study authored by a researcher from the National Institute of Standards and Technologies, which tests facial recognition products every four years, found that while accuracy rates[89] have improved over the years, accurate recognition is affected by the racial compositions of an algorithm's development team and the database of test photos.[90] This means that, for example, algorithms developed in Germany more accurately identify Caucasians while algorithms developed in Japan are better at identifying East Asians.[91] In the melting pot of the United States, however, the algorithms were "significantly better at recognizing Caucasian facial characteristics."[92] A 2012 study of facial recognition algorithms used by U.S. law enforcement "found that the algorithms were 5–10% less accurate when reading black faces over white ones and showed similar discrepancies when analyzing faces of women and younger people,"[93] and additional studies have found errors up to thirty-five percent of the time for images of darker skin.[94] This flaw in facial recognition algorithms has the potential to compound existing biases, particularly in light of law enforcement's already disproportionate mistreatment of Black people.[95] Since misidentifications of people of color lead to unnecessary interactions with the police, and given the police are more likely to use force on people of color, it follows that misidentification could lead to further harm.[96]

89. The "accuracy rate" of a facial recognition algorithm is the rate at which the technology accurately matches a face image to the database.

90. Garvie & Frankle, *supra* note 86.

91. *Id*.

92. *Id*.

93. Couch, *supra* note 68.

94. Steve Lohr, *Facial Identification Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html [https://perma.cc/EY7H-MNDE (dark archive)]. In contrast, identification of White men is accurate up to ninety-nine percent of the time. *Id*.

95. *See* Devon W. Carbado & L. Song Richardson, *The Black Police: Policing Our Own*, 131 HARV. L. REV. 1979, 1992–95 (2018) (describing the impact of implicit bias resulting in disproportionate mistreatment of Black people in policing, even by Black police officers); Quoctrung Bui & Amanda Cox, *Surprising New Evidence Shows Bias in Police Use of Force but Not in Shootings*, N.Y. TIMES (July 11, 2016), https://www.nytimes.com/2016/07/12/upshot/surprising-new-evidence-shows-bias-in-police-use-of-force-but-not-in-shootings.html [https://perma.cc/Z6F6-M7EB (dark archive)] (explaining that while one study found no racial bias in police shootings, it did find that police officers are more likely to use certain kinds of force against Black men than against other suspects: Black men are "more likely to be touched, handcuffed, pushed to the ground or pepper-sprayed by a police officer"); German Lopez, *There Are Huge Racial Disparities in How US Police Use Force*, VOX (Nov. 14, 2018), https://www.vox.com/identities/2016/8/13/17938186/police-shootings-killings-racism-racial-disparities [https://perma.cc/4W38-HHYX] ("Black people accounted for 31 percent of police killings in 2012, even though they made up just 13 percent of the US population.").

96. Bui & Cox, *supra* note 95; *see also* Kaitlyn Burton, *Amazon Investors To Vote on Halting Face Recognition Sales*, LAW360 (Apr. 5, 2019), https://www.law360.com/corporate/articles/1146819/amazon-investors-to-vote-on-halting-face-recognition-sales [https://perma.cc/6PL8-NQYX (dark

2. Machine Bias in Schools

In the context of K-12 schools, these biases are even more problematic. Students of color are already subjected to disproportionate disciplinary action in K-12 schools,[97] which ultimately places them at higher risk for entry into the criminal justice system via the "school-to-prison pipeline."[98] Inserting a flawed surveillance system into the mix could further threaten access to education for students of color, ultimately impacting their economic success and physical health.[99] Further, facial detection readings of women's faces are often inaccurate.[100] Currently, "Black girls face high and disproportionate suspension rates across the country—and it's not because they are misbehaving more frequently than other girls."[101] Rooted in implicit bias and stereotyping, Black girls are held to "lower academic expectations" and "make up disproportionately high shares of girls who are retained in every single grade."[102] Thus, it is not much of a leap to anticipate a disproportionate number of instances where Black girls are misidentified by facial recognition technology, such as a situation where a school is looking at surveillance of a fight or another conduct violation. This misidentification could result in disciplinary and negative academic

archive)] ("Critics have said the [Amazon facial recognition] technology could be used to spy on minorities, such as undocumented immigrants or African-American activists.").

97. *See* Tom Loveless, *Racial Disparities in School Suspensions*, BROOKINGS (Mar. 24, 2017), https://www.brookings.edu/blog/brown-center-chalkboard/2017/03/24/racial-disparities-in-school-suspensions/ [https://perma.cc/B2F9-MMXQ] ("Suspensions of African American students occur at rates three to four times higher than the state average for all students.").

98. AM. BAR ASS'N, ABA TASK FORCE ON REVERSING THE SCHOOL-TO-PRISON PIPELINE 10 (2018), https://www.americanbar.org/content/dam/aba/images/racial_ethnic_justice/Final%20School2PrisonPipeline-2nd-012618.pdf [https://perma.cc/T33B-X76H] ("According to the U.S. Department of Education's Office of Civil Rights, discipline and other disparities are based on race and cannot be explained by more frequent or serious misbehavior by minority students."); *School Discipline and the School-to-Prison Pipeline*, ANTI-DEFAMATION LEAGUE, https://www.adl.org/education/resources/tools-and-strategies/table-talk/school-to-prison-pipeline [https://perma.cc/JQ52-2D3L] ("Largely as a result of 'zero tolerance' policies that mandate harsh punishments for even minor misbehavior in schools, 3.3 million children are suspended or expelled from school each year, about double the rate of the 1970s.").

99. Students of color who do not complete high school receive lower salaries than their White dropout counterparts. NAT'L WOMEN'S LAW CTR., WHEN GIRLS DON'T GRADUATE WE ALL FAIL 8 (2007), https://nwlc-ciw49tixgw5lbab.stackpathdns.com/wp-content/uploads/2015/08/when_girls_dont_graduate.pdf [https://perma.cc/2C7T-9F46]. Students of color are less likely to complete high school than White students. AM. PUB. HEALTH ASS'N, THE DROPOUT CRISIS: A PUBLIC HEALTH PROBLEM AND THE ROLE OF SCHOOL-BASED CARE 2 (Feb. 2018), https://www.apha.org/-/media/files/pdf/sbhc/dropout_crisis [https://perma.cc/XM77-DEVF]. Individuals who do not attain a high school education "are more likely to die prematurely from preventable conditions." *Id.*

100. Couch, *supra* note 68.

101. Lauren Camera, *Black Girls Are Twice As Likely To Be Suspended, in Every State*, U.S. NEWS & WORLD REP. (May 9, 2017), https://www.usnews.com/news/education-news/articles/2017-05-09/black-girls-are-twice-as-likely-to-be-suspended-in-every-state [https://perma.cc/7357-95LR].

102. NAT'L WOMEN'S LAW CTR., LET HER LEARN: STOPPING SCHOOL PUSHOUT FOR GIRLS OF COLOR 3 (2017), https://nwlc.org/wp-content/uploads/2017/04/final_nwlc_Gates_GirlsofColor.pdf [https://perma.cc/7TV4-FYKY].

consequences. If this technology is used to determine who was involved in a conduct incident or who is permitted to enter the school, students of color will be at risk of being misidentified as individuals who committed conduct violations or are otherwise prohibited from entry.

Research also indicates that facial recognition technology has high rates of inaccurate identification of younger faces,[103] one of the target populations of these scans in schools. There is no information regarding how accurately facial recognition technology identifies developing faces. An eighth-grade student may look very different at the end of a school year compared to the beginning of the year, and teenagers, especially, tend to change their appearances. It is not clear whether districts and these machines will be able to keep up.[104] Given the uncertainty around accurate identification of young people, a threat of negative impact on the academic environment remains. All students should feel comfortable operating in their academic institutions without experiencing embarrassment due to an erroneous identification or fearing interactions with law enforcement.

If a child is misidentified by a machine, surely a human administrator should be able to confirm the machine's read before taking further action, but such confirmation may still require that the student be pulled from class for questioning. Perhaps after a fight in the hall, a camera identifies student *X* as the culprit and the principal pulls that student from class to address the conduct violation, but student *X* was misidentified. Even if an administrator ultimately finds the identification to be inaccurate—perhaps student *X* was not even at school that day—the harm of removing a student from class or making a damning allegation against them is already done. What happens when a child's parent is misidentified? The resulting stigma could profoundly impact a young person, who may be embarrassed and confused. Bullying in K-12 schools is common,[105] and a student or parent being questioned or detained could lead to bullying, making the academic environment unsafe and unwelcoming for that student. Alternatively, fear of misidentification could lead caregivers to avoid basic school functions, such as parent-teacher conferences, which may have further deleterious effects on a child's education. These are questions that, as of

103. Couch, *supra* note 68.

104. Emily Ann Brown, *Biometric Security Boosts School Safety and Efficiency*, DISTRICT ADMIN. (Mar. 19, 2019), https://districtadministration.com/biometric-security-boosts-school-safety-efficiency/ [https://perma.cc/CEA2-UWPK] ("Unlike finger scans, students' faces change as they grow. Creating and 'cleaning' a database requires more effort, says Sara Collins, policy counsel for the Education Privacy Project at the Future of Privacy Forum.").

105. Amy Rock, *Bullying Statistics Every K-12 Teacher, Parent and Student Should Know*, CAMPUS SAFETY MAG. (Dec. 10, 2018), https://www.campussafetymagazine.com/safety/bullying-statistics-k-12/ [https://perma.cc/8D46-83TK] (reporting results from a 2016 National Center for Education Statistics study that found that one in five students reported being bullied).

now, appear to have no concrete answers but must be addressed before these technologies are implemented for surveillance in K-12 environments.

An example of AI surveillance technology in a K-12 setting is Lockport City School District in New York, which contracted with a security company to install a high-tech system with facial recognition.[106] The district was slammed by parents and privacy advocates with concerns that the software would misidentify students and negatively affect the school climate.[107] The school district planned to only upload images of individuals prohibited from entry or students flagged for disciplinary issues,[108] but the system would still scan every child for comparison against the database.[109] Further, the video surveillance feature would have beefed up school discipline, allowing school officials to upload a student photo and then track the student in the video system to evaluate a disciplinary incident.[110] This harkens back to the concerns regarding the likely disproportionate impact on students of color. After paying $1.4 million, contracting with the security company, and installing the camera systems, the school district finally yielded to its critics and updated the school security policy to reflect privacy protections.[111] The changes include limiting access to the database to a few individuals with high security clearances, not maintaining any alerts resulting from misidentification in students' records, and providing weekly updates to the Board of Education containing the names of individuals added to the database.[112]

Given all of the potential harms, schools should be concerned when implementing advanced technologies for surveillance purposes. However, they may also need to be worried about liability if they do not implement advanced surveillance technologies. The proliferation of these technologies leaves open questions about school liability under a negligence theory if a school declines to implement available technologies. The question remains: If the technology is available and school officials do not opt into using it, or misuse it, who is at fault if there is a shooting at the school? Due to this potential for liability, schools may be further incentivized to employ such technologies. Moreover, given that

106. Prohaska, *Beef Up Security*, *supra* note 23.

107. Amy Rock, *School Districts Consider Facial Recognition To Improve Security*, CAMPUS SAFETY MAG. (July 26, 2018), https://www.campussafetymagazine.com/safety/school-districts-facial-recognition/ [https://perma.cc/Z6KG-9FWD].

108. Prohaska, *Beef Up Security*, *supra* note 23.

109. Mariella Moon, *Facial Recognition Is Coming to U.S. Schools, Starting in New York*, ENGADGET (May 30, 2019), https://www.engadget.com/2019/05/30/facial-recognition-us-schools-new-york/ [https://perma.cc/YE4U-GM3G].

110. Prohaska, *Beef Up Security*, *supra* note 23.

111. Connor Hoffman, *Lockport School Officials Update Security Policies Related to Facial Recognition Software*, LOCKPORT J. (Feb. 10, 2019), https://www.lockportjournal.com/news/local_news/lockport-school-officials-update-security-policies-related-to-facial-recognition/article_41b1f38b-ad28-508a-982f-6936641d2307.html [https://perma.cc/6UDT-TV2U].

112. *Id.*

privacy laws are malleable at best, and there is not much in terms of legal protection against bias, most of the incentives in this decision tend to encourage schools to rush into using technologies without fully considering the risks or harms.

III. PRIVACY LAWS AND SCHOOL SURVEILLANCE

There has been little exploration into the privacy implications of advanced surveillance technologies in schools. This part provides background on several privacy laws that already are, or very likely will be, applied to advanced surveillance technologies in schools. It also argues that the appropriate actors must clarify how these laws will apply to new technologies in order to inform potential consumers about the risks they are facing. When it comes to these technologies, the implementing authorities will undoubtedly have to navigate a wide variety of laws that protect the privacy of schoolchildren.

Students are protected—to a certain extent—by the Fourth Amendment.[113] FERPA governs the protection of student records[114] but is currently limited in its ability to regulate information obtained from these advanced technologies. Furthermore, a handful of states have begun passing laws to protect students from biometric information gathering, and these state laws are likely the most realistic and efficient path forward to privacy protection.[115] As Louis Brandeis and Samuel Warren predicted in their seminal 1890 paper *The Right to Privacy*, "Political, social, and economic changes entail the recognition of new rights."[116] Similarly, today's surveillance state is altering society to the point that privacy rights must be extended to children in schools who are under the watchful eye of AI and biometrics.

A. *The Fourth Amendment*

1. The Supreme Court's Approach to Intangible Searches

Supreme Court jurisprudence applying the Fourth Amendment to emerging technologies is limited but creates a potential framework for evaluating AI in schools. Interpretation of the Fourth Amendment was

113. *See infra* Section III.A.

114. *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T EDUC. (Mar. 1, 2018) [hereinafter *FERPA*, U.S. DEP'T EDUC.], https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html [https://perma.cc/DC2R-HADE].

115. *See* Andrew Ujifusa, *State Lawmakers Ramp Up Attention to Data Privacy*, EDUC. WK. (Apr. 15, 2014) [hereinafter Ujifusa, *Ramp Up Attention*], https://www.edweek.org/ew/articles/2014/04/16/28data.h33.html [https://perma.cc/4QLB-P8B9 (dark archive)] (providing an overview of biometric data laws that impact schools in Florida and Kansas); *see also* discussion *infra* Section III.B.

116. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

historically limited to a physical conception of privacy invasion and has been slow to catch up to technological advancements. In 1928, the Supreme Court ruled in *Olmstead v. United States*[117] that the protections of the Fourth Amendment did not apply to wiretapping and that the amendment does not apply "unless there has been an official search and seizure of [a] person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[118] However, in his scathing dissent, the forward-thinking Justice Brandeis challenged the majority's hesitance to consider technological advances:

> "[I]n the application of a constitution, our contemplation cannot be only of what has been, but of what may be." . . . Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[119]

It took nearly forty years for the Supreme Court to overturn *Olmstead*[120] and catch up to rapidly advancing technological progress as Justice Brandeis had urged. In 1967, the Court held in *Katz v. United States*[121] that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure," and thus the government's wiretapping of a phone booth "constituted a 'search and seizure' within the meaning of the Fourth Amendment."[122] The resulting updated framework for determining whether something is a search came not from the majority opinion but from Justice Harlan's concurrence.[123] This two-pronged "*Katz* test" asks whether (1)

117. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

118. *Id.* at 466 ("We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.").

119. *Id.* at 474 (Brandeis, J., dissenting). Justice Brandeis's opinion was much in line with the paper he published in 1890. *See* Warren & Brandeis, *supra* note 116, at 193 ("[T]he term 'property' has grown to comprise every form of possession—intangible, as well as tangible.").

120. *See* Katz v. United States, 389 U.S. 347, 353 (1967) ("[A]lthough a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1960))).

121. 389 U.S. 347 (1967).

122. *Id.* at 353.

123. *See id.* at 360–62 (Harlan, J., concurring).

the "person [has] exhibited an actual (subjective) expectation of privacy" and (2) the "expectation [is] one that society is prepared to recognize as 'reasonable.'"[124] The test was quickly adopted by the full Court as the standard for assessing Fourth Amendment cases and continues to be used today.[125]

Despite this crucial development in Fourth Amendment jurisprudence, laws regulating intangible surveillance technologies still face uncertainty in the courts.[126] Most recently, the Court held in a splintered decision in *Carpenter v. United States*[127] that the Fourth Amendment protects historical cell-site location information ("CSLI").[128] Cell-sites are radio towers that connect a phone to the wireless network, and the resulting CSLI is a time-stamped record generated from a phone connecting to the wireless network that places an individual near that particular cell-site at the times recorded.[129] Wireless carriers retain CSLI as business records,[130] but in *Carpenter* a court had ordered MetroPCS and Sprint to disclose the CSLI of individuals suspected of a robbery.[131] The CSLI placed the suspect's phone near the robbery by showing that the phone was pinging off of cell-sites surrounding the crime scene at the time of the crime.[132] After the defendant was convicted, the case made its way to the Supreme Court, where the defendant argued that he had a reasonable expectation of privacy to his CSLI.[133] The Justices took different approaches to the Fourth Amendment inquiry, disagreeing about which privacy test to use and whether CSLI should be considered protected at all.[134] The result of *Carpenter* did not provide a simple

124. *Id.* at 361.

125. *See* Mancusi v. DeForte, 392 U.S. 364, 368 (1968) (citing *Katz* in employing a "reasonable expectation" of privacy standard, merely one year after the *Katz* decision); *see also* Kyllo v. United States, 533 U.S. 27, 33 (2001) ("As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring))); Smith v. Maryland, 442 U.S. 735, 740 (1979) ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action.").

126. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012) (holding that the installation of a GPS device on defendant's car was a search under the Fourth Amendment); Everett v. State, 186 A.3d 1224, 1236 (Del. 2018) (holding that the defendant did not have a reasonable expectation of privacy when posting photographs on social media). *But see* United States v. James, No. 18-cr-216, 2018 WL 6566000, at *4 (D. Minn. Nov. 26, 2018) (declining to address the issue of whether a person has a reasonable expectation of privacy as to cell tower records that differ from those narrowly addressed in *Carpenter*).

127. 138 S. Ct. 2206 (2018).

128. *Id.* at 2221.

129. *Id.* at 2211.

130. *Id.* at 2212.

131. *Id.*

132. *Id.* at 2212–13.

133. *See id.*

134. *See id.* at 2219 (applying the reasonable expectation of privacy test); *id.* at 2224 (Kennedy, J., dissenting) (explaining that the property-based test should be applied because property-based concepts

test going forward; in fact, the Court specified that its decision was a "narrow one."[135] Schools looking to *Carpenter* to answer questions about what is protected under the Fourth Amendment may gain some insights but have no assurances about the degree to which it applies to AI surveillance.

2. *T.L.O.*'s Two-Pronged Test for Searches in Schools

In the context of schools, the extent to which the Fourth Amendment protects privacy is a complicated issue. The Fourth Amendment is made applicable to public schools through the Fourteenth Amendment[136] and, to a certain extent, protects students from unreasonable searches and seizures in school. In the 1985 landmark case *New Jersey v. T.L.O.*,[137] the Supreme Court addressed whether the Fourth Amendment's "prohibition on unreasonable searches and seizures applies to searches conducted by public school officials."[138] After holding that the Fourth Amendment applies to school officials as state actors, the Court set forth a relaxed, two-part framework for analyzing searches by school officials: the first question asks whether the search was "justified at its inception," and the second asks whether the search was reasonable in scope.[139]

The Court explained that "a search [by school officials] will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction."[140] The two-pronged test was derived from the "reasonable suspicion" standard the Court set forth in *Terry v. Ohio*.[141] The Court did not require probable cause for searches in schools because it concluded that the reasonableness standard would "neither unduly burden the efforts of school authorities to maintain order in their schools nor authorize unrestrained intrusions upon the privacy of schoolchildren."[142] The *T.L.O.* decision was a turning point in jurisprudence about school discipline because it established a Fourth Amendment framework and consequently shifted the landscape of school security.

---

have "long grounded the analytical framework" of Fourth Amendment cases); *id.* at 2264 (Gorsuch, J., dissenting) (advocating for a textual-based approach by arguing that the plain language of the Fourth Amendment should ultimately determine the outcome of the case).

135. *Id.* at 2220 (majority opinion) ("We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras.").

136. *See* New Jersey v. T.L.O., 469 U.S. 325, 334 (1985) (holding that the actions of public school officials are subject to the limits placed on state action by the Fourteenth Amendment).

137. 469 U.S. 325 (1985).

138. *Id.* at 333.

139. *Id.* at 341.

140. *Id.* at 342.

141. *Id.* at 341 (citing Terry v. Ohio, 392 U.S. 1, 20 (1968)).

142. *Id.* at 342–43.

While there have not been many opportunities for courts to grapple with the appropriateness and constitutionality of various forms of electronic surveillance in schools,[143] the relationship between intangible searches, as addressed in *Katz*, and searches in schools, as addressed in *T.L.O.*, came to a head as recently as 2008. In the Sixth Circuit case *Brannum v. Overton County School Board*,[144] officials at a public middle school installed video cameras throughout the school, including in locker rooms.[145] A group of students sued, arguing that "their constitutionally protected right to privacy encompasses the right not to be videotaped while dressing and undressing in school athletic locker rooms—a place specifically designated by the school authorities for such intimate, personal activity."[146]

With no Supreme Court or Sixth Circuit cases on point, the *Brannum* court utilized the *T.L.O.* framework.[147] In determining that the installation of surveillance cameras passed *T.L.O.*'s justified-at-inception prong, the court stated that "the policy of setting up video surveillance equipment throughout the school was instituted for the sake of increasing security, which is an appropriate and common sense purpose."[148] However, the school crossed the line of Fourth Amendment limitations regarding the scope of the search. According to the *Brannum* court, the search was unreasonable in scope because "even in locker rooms, students retain 'a significant privacy interest in their unclothed bodies.'"[149] While the Sixth Circuit's ruling may have been unsurprising because videotaping minors in various stages of undress seems innately wrong, the court's rationale was not so narrow as to limit the decision's implications to similar situations. The Sixth Circuit instead took a broad approach, asserting that "[v]ideo surveillance is *inherently* intrusive."[150] Under this reasoning, regardless of its location or the level of intimacy it may capture, video surveillance raises privacy concerns.

Five years later in *G.C. v. Owensboro Public Schools*,[151] the Sixth Circuit again found itself applying the *T.L.O.* framework and *Brannum* principles, this time to determine whether a school official violated the Fourth Amendment

143. This is unsurprising given that this is a new issue, the rate at which technology is developing, and the Supreme Court's aversion to questions about technology. *See* Amelia Thomson-DeVeaux, *The Supreme Court Is Stubbornly Analog—By Design*, FIVETHIRTYEIGHT (May 29, 2018) https://fivethirtyeight.com/features/the-supreme-court-is-stubbornly-analog-by-design/ [https://perma.cc/VX6E-LD2C] ("The Supreme Court is an openly—even proudly—technophobic institution.").

144. 516 F.3d 489 (6th Cir. 2008).

145. *Id.* at 492.

146. *Id.* at 494.

147. *Id.* at 494–95.

148. *Id.* at 496.

149. *Id.* (quoting Beard v. Whitemore Lake Sch. Dist., 402 F.3d 598, 604 (6th Cir. 2005)).

150. *Id.* (emphasis added).

151. 711 F.3d 623 (6th Cir. 2013).

when she confiscated a student's cell phone and read his text messages.[152] In a decision rooted in the *T.L.O.* two-pronged reasonableness framework, the court declined to approve of the search, finding that "using a cell phone on school grounds does not automatically trigger an essentially unlimited right enabling a school official to search any content stored on the phone that is not related either substantively or temporally to the infraction."[153] Here, the Sixth Circuit focused primarily on the justified-at-inception prong of the *T.L.O.* framework when finding that "[t]he defendants have failed to demonstrate how anything in this sequence of events indicated to them that a search of the phone would reveal evidence of criminal activity, impending contravention of additional school rules, or potential harm to anyone in the school."[154] *G.C.* did not involve electronic surveillance in the context of cameras, but by searching the phone, the school was able to acquire information about the student that they would not have been able to obtain without the technology. The court applied Fourth Amendment principles in the context of a form of technology that is used with increasing frequency, indicating the judiciary's willingness to apply Fourth Amendment principles to modern technology in the school context. It sheds light on the ways in which courts are approaching schools' searches of students using technology as a medium.[155]

3. Complexities of Applying the *T.L.O.* Framework to AI Surveillance

These cases indicate that courts will likely apply the *T.L.O.* framework to Fourth Amendment challenges to school surveillance programs, but uncertainty remains. As Justice Brandeis anticipated in his *Olmstead* dissent,[156] courts and lawmakers have been hesitant to take positions on emerging technologies that have the potential to implicate privacy.[157] If the "inherently intrusive" argument from *Brannum* is widely applied, it could significantly limit the scope of video surveillance in schools.[158] However, it remains to be seen whether jurisdictions beyond the Sixth Circuit will adopt that view; courts have not yet considered many cases involving the implication of student rights under the Fourth

152. *Id.* at 626, 632.

153. *Id.* at 632–33.

154. *Id.* at 634; *see* New Jersey v. T.L.O., 469 U.S. 325, 341–2 (1985) (explaining that a search will be "justified at its inception" when there are reasonable grounds for suspecting the search will reveal a violation of the law or school rules).

155. *See Know Your Rights: Student Cell Phone Privacy*, AM. C.L. UNION N. CAL., https://www.aclunc.org/our-work/know-your-rights/student-cell-phone-privacy [https://perma.cc/S4DS-WX5L].

156. *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

157. *See infra* Section III.C (presenting an overview of current state laws).

158. *But see* Marriott v. USD 204, Bonner Springs-Edwardsville, 289 F. Supp. 3d 1235, 1240 (D. Kan. 2017) (holding there is no reasonable expectation of privacy in a classroom because it is a public place).

Amendment and particularly have not addressed questions of school surveillance.

Notably, *Brannum* and *G.C.* were wins for student rights, but the *T.L.O.* standard remains a relaxed application of the Fourth Amendment and is thus more susceptible to interpretations that weaken protections of student privacy. While *T.L.O.* held that school officials are considered state actors and are obligated to act within the parameters of the Fourth Amendment when conducting searches in schools, the Court also endorsed the lesser "reasonable suspicion" prerequisite for searches conducted by school officials.[159] In contrast to school officials, police officers generally must have "probable cause" to conduct a search or seizure.[160] The intersection of *T.L.O.* and the increase of surveillance mechanisms in schools therefore may lead to confusion with respect to how these requirements apply to school resource officers,[161] who are law enforcement officers but work in a capacity similar to school officials.[162] In *People v. Dilworth*,[163] the Illinois Supreme Court categorized school search cases involving the police and found that "most courts have held that the reasonable suspicion test" applies where "school officials initiate a search or where police involvement is minimal" and in situations "involving school police or liaison officers acting on their own authority."[164] However, "where outside police officers initiate a search," courts typically require probable cause.[165] *Dilworth* provides a helpful survey of court opinions, but as a state court case, its determinations are not binding outside of its limited jurisdiction.

Since there is no clear answer regarding the Fourth Amendment implications of existing security mechanisms in schools, evolving AI systems raise even more confusion. The justified-at-inception prong of the search may look different in the AI context. For example, it is unclear whether a facial recognition camera's alert to a school administrator that someone on the blacklist has entered campus would meet the requirement. Furthermore, the biometric scanning of students each time they walk through a different door in the school building may reach beyond a "reasonable scope" under the framework because scanning children's faces multiple times per day may be "excessively

159. *T.L.O.*, 469 U.S. at 345; *see supra* text accompanying notes 141–42.

160. U.S. CONST. amend. IV. When an officer has only reasonable suspicion, rather than probable cause, that an individual is armed, about to commit a crime, or engaged in a crime, the officer may "stop and frisk" the individual, which involves a brief detention and a pat-down. Terry v. Ohio, 392 U.S. 1, 24–26 (1968).

161. Bernard James, *Student Searches: Part II: Fine-Tuning the Educator/SRO Relationship*, J. SCH. SAFETY (2008), https://nasro.org/cms/wp-content/uploads/2017/11/Student-Searches-JOSS-Summer-2008.pdf [https://perma.cc/62MK-H6SM].

162. *Frequently Asked Questions*, NAT'L ASS'N SCH. RESOURCE OFFICERS, https://nasro.org/frequently-asked-questions/ [https://perma.cc/GU6J-23V7].

163. 661 N.E.2d 310 (Ill. 1996).

164. *Id.* at 317.

165. *Id.*

intrusive." Schools and law enforcement may very well be opening themselves up to liability under the Fourth Amendment for conducting improper searches. Without further guidance from the courts, which likely will not come for a while, many of these technologies will likely cause inconsistencies across schools in how the *T.L.O.* framework is applied.

B. *FERPA*

The Fourth Amendment is not the only limiting factor on the potential breadth of use of AI surveillance technologies. Congress has also stepped in to protect schoolchildren's privacy. FERPA is a federal law that "protects the privacy of student education records" and "gives parents certain rights with respect to [those] records."[166] Generally, FERPA prevents schools from sharing "personally identifiable information," which is distinguished from "directory information."[167] FERPA may be traditionally viewed as governing disciplinary records or specific grades but in most situations includes photos and videos of students as part of the protected education record.[168]

Despite its ostensible purpose to protect student privacy, there is little certainty as to whether or how FERPA protects student data collected through forms of AI surveillance. Outside of a plain reading of the student privacy law, there are many exceptions to FERPA protection. These include two exceptions relevant to the school surveillance context: the "health or safety exception"[169] and the "school officials exception."[170] These exceptions allow schools, in some cases, to distort the original intent of the law and disclose information that should remain private.

Two dichotomous problems are often raised in the context of FERPA: (1) FERPA is not stringent enough and allows education agencies to disclose too much information without consent,[171] and (2) FERPA is used as a shield by

166. *FERPA*, U.S. DEP'T EDUC., *supra* note 114; *see also* 20 U.S.C. § 1232g (2012 & Supp. IV 2016).

167. § 1232g(a)(5)(A), (b)(2) ("[T]he term 'directory information' relating to a student includes the following: the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.").

168. *See FAQs on Photos and Videos Under FERPA*, U.S. DEP'T EDUC., https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa [https://perma.cc/G6YY-298C].

169. *See infra* Section III.B.2.

170. *See infra* Section III.B.3.

171. Benjamin Herold, *Arne Duncan Responds to Criticism Over Student Data Privacy*, EDUC. WK. (Apr. 15, 2014), https://blogs.edweek.org/edweek/DigitalEducation/2014/04/duncan_on_data_privacy_technol.html [https://perma.cc/QSF9-FN8C (dark archive)] ("Some privacy advocates, including Khaliah Barnes, a lawyer for the Washington-based nonprofit Electronic Privacy Information Center, argue that FERPA is too outdated and weak to protect children's information in this era of big data and ubiquitous digital devices and tools."); Jake New, *Staying Confidential*, INSIDE HIGHER ED.

education agencies to hide information they do not want to reveal to the public.[172] With respect to the second criticism, some groups in recent years have criticized schools' use of FERPA as a shield to cover up wrongdoing and hide from bad publicity.[173] Even the original sponsor of the law, former Senator James L. Buckley, recently called out "a pattern where the universities and colleges have used [FERPA] as an excuse for not giving out any information they didn't want to give."[174] When it comes to AI, these issues will only become more complex, and, without Congress strengthening FERPA, much of the collected information will be at risk of disclosure.

1. Development of FERPA

Congress passed FERPA in 1974 with the intention of protecting students.[175] The law was originally passed with little discussion, but after public backlash, the bill's sponsors issued a statement "emphasiz[ing] the need for parents to have access to the information contained in student education records in order to protect their children's interests."[176] FERPA was subsequently amended to explicitly protect the privacy of students' personally identifiable information by "strengthen[ing] the right of students to a hearing to challenge the content of records they believe are inaccurate, misleading, or otherwise in

(Aug. 3, 2015), https://www.insidehighered.com/news/2015/08/03/privacy-loophole-remains-open-after-outrage-over-u-oregons-handling-therapy-records [https://perma.cc/P222-RMU2].

172. Amye Bensenhaver, *Kentucky Universities Continue To Hide Behind FERPA*, FORWARD KY. (June 12, 2019), https://forwardky.com/kentucky-universities-continue-to-hide-behind-ferpa/ [https://perma.cc/QM5L-BZKS]; Frank D. LoMonte, *Ferpa Frustrations: It's Time for Reform*, CHRON. HIGHER EDUC. (May 9, 2010), https://www.chronicle.com/article/Ferpa-Frustrations-Its-Time/65419 [https://perma.cc/WEF2-6KJU (dark archive)].

173. Zach Greenberg, *Let Ferpa Be Ferpa*, CHRON. HIGHER EDUC. (Jan. 14, 2018), https://www.chronicle.com/article/Let-Ferpa-Be-Ferpa/242232 [https://perma.cc/Y9U3-ZT7A (dark archive)] ("[FERPA] has been invoked to stifle police investigations into campus crime and cover up scandal after scandal concerning college athletics, cronyism in admissions practices, and administrative malfeasance."); Tamar Lewin, *Privacy and Press Freedom Collide in University Case*, N.Y. TIMES (Oct. 20, 2011), https://www.nytimes.com/2011/10/21/education/21privacy.html [https://perma.cc/TC28-MAHT (dark archive)] (discussing a legal battle between the University of Illinois and The Chicago Tribune over documents related to the university's longstanding admission of well-connected students: "The Tribune, backed by media groups including The New York Times, argues that the documents are not education records under the federal law, but rather records of questionable conduct, so the public's right to know should prevail"); George Schroeder, *It's Clear the 'O' Stands for Opaque*, REGISTER-GUARD (Feb. 18, 2011), http://special.registerguard.com/csp/cms/sites/web/sports/columnists/25904339-41/records-public-ncaa-oregon-ferpa.csp [https://perma.cc/6TVQ-LHTQ] (discussing the University of Oregon's denial of a newspaper's open-records request where one journalism professor called the university's denial "an abuse of FERPA to conceal records of an NCAA investigation into possible rules violations by student athletes").

174. Schroeder, *supra* note 173.

175. *See* 121 CONG. REC. 13,990 (1975) (remarks of Sen. Buckley).

176. *Family Educational Rights and Privacy Act (FERPA)*, ELECTRONIC PRIVACY INFO. CTR. [hereinafter *FERPA*, ELECTRONIC PRIVACY INFO CTR.], https://epic.org/privacy/student/ferpa/ [https://perma.cc/VD5L-ARVT].

violation of their privacy or other rights."[177] The law has been amended a number of times to account for new issues.[178] However, the Department of Education weakened FERPA in 2008 through rulemaking in spite of opposition by privacy advocates and civil liberties groups.[179] The 2008 rule amended FERPA regulations to "authorize the disclosure of education records without consent to contractors, consultants, volunteers, and other outside parties to whom an educational agency or institution has outsourced institutional services or functions."[180]

In recent years, there have been demands for the U.S. Department of Education to issue guidance to clarify FERPA's scope and application, and some critics have pressured Congress to update the law to meet new security and privacy needs created by advanced technology.[181] Although the 2008 rule received flak for its expansion of record disclosure, it did expand the definition of "personally identifiable information" to include biometric data under the statute.[182] The rule clarified that a student's biometric record includes "fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting."[183] This update was a vital step in protecting students from disclosure of personal information obtained through advanced

177. *Id.*; *see* Act of Dec. 31, 1974, Pub. L. No. 93-568, sec. 2(4)(A), § 438(a)(2), 88 Stat. 1855, 1861 (codified as amended at 20 U.S.C. § 1232g(a)(2) (2012 & Supp. IV 2016)).

178. *See FERPA*, ELECTRONIC PRIVACY INFO. CTR., *supra note* 176 (listing the nine amendments to FERPA since its enactment); *see also* 20 U.S.C. § 1232g (2012 & Supp. IV 2016).

179. *See, e.g.*, Letter from Laura W. Murphy, Dir., Wash. Legislative Office, Am. Civil Liberties Union, & Christopher R. Calabrese, Legislative Counsel, Am. Civil Liberties Union, to Regina Miles, U.S. Dep't of Educ. (May 23, 2011), https://www.aclu.org/files/assets/ACLU_Comments_on_Changes_to_the_Family_Educational_Rights_and_Privacy_Act_FERPA.pdf [https://perma.cc/G5BC-9LRV] ("This notice of proposed rulemaking (NPRM) represents a significant new privacy invasion."); ELEC. PRIVACY INFO. CTR., COMMENTS OF ELECTRONIC PRIVACY INFORMATION CENTER TO THE DEPARTMENT OF EDUCATION (May 23, 2011), https://epic.org/privacy/student/EPIC_FERPA_Comments.pdf [https://perma.cc/U4SX-BKJB] ("Expanding third party access to student data is contrary to FERPA, given the purpose of the Act.").

180. Family Educational Rights and Privacy, 73 Fed. Reg. 74,806, 74,806 (Dec. 9, 2008) (codified as amended at 34 C.F.R. § 99.31(a)(1) (2019)).

181. *See* Greenberg, *supra* note 173; Henry Kronk, *Student Data Security Is at Risk. We Need To Update FERPA*, ELEARNING INSIDE (Nov. 25, 2018), https://news.elearninginside.com/student-data-security-is-at-risk-we-need-to-update-ferpa/ [https://perma.cc/GQM7-G7FF]; Andrew Ujifusa, *School Officials Urge Congress to Update Student-Data Privacy Law*, EDUC. WK. (May 17, 2018), http://blogs.edweek.org/edweek/campaign-k-12/2018/05/school_officials_student_data_privacy_law_congress_urge.html [https://perma.cc/GRY9-TSMT (dark archive)]; *see also* Benjamin Herold, *Trump School Safety Commission: Time To Update FERPA*, EDUC. WK. (Dec. 18, 2018), https://blogs.edweek.org/edweek/DigitalEducation/2018/12/school_safety_commission_ferpa.html [https://perma.cc/CVK9-KG7U (dark archive)].

182. Family Educational Rights and Privacy, 73 Fed. Reg. at 74,851 (codified as amended at 34 C.F.R. § 99.3(d) (2019)).

183. *Id.*

technologies. Nonetheless, all personally identifiable information, including biometric information, may be disclosed if it falls within a FERPA exception.

2. The "Health or Safety Exception" and Surveillance

As part of its 2008 rule, which was promulgated one year after the mass shooting at Virginia Tech,[184] the Department of Education clarified when typically protected student information may be disclosed for health or safety reasons.[185] The "health or safety exception," as it is called, gives schools "greater flexibility and deference" to disclose educational records without consent to "appropriate parties," which could include law enforcement or emergency responders, among others.[186] The exception may be employed in the presence of an "actual, impending, or imminent emergency"—including "a campus shooting"—and any information released must be related to the emergency.[187]

The Department's recently released School Safety Commission Final Report demonstrates that the boundaries of the health and safety exception are less than clear; schools remain confused about when FERPA protects safety-related student information and when that information falls within the exception.[188] The Department's report explained that law enforcement officers who "[sought] access to school surveillance footage to help ensure school safety" were denied access by schools that claimed the footage was protected by FERPA.[189] The officers in those cases believed that FERPA permitted them to access the footage.[190] In an attempt to dispel this confusion, the Department explained, "If a school's security department or campus police maintains the school's surveillance video system and, as a result, creates surveillance footage for a law enforcement purpose, FERPA would not prevent sharing the surveillance footage with local law enforcement."[191]

The report does not clear up all of the confusion surrounding FERPA information-sharing permissions as applied to surveillance technologies. The Department's explanation seems to consider all school surveillance footage to be for a law enforcement purpose and thus shareable under the exception.[192] Moreover, the report specifies that a school official can be designated "as the

184. *See* Hauser & O'Connor, *supra* note 1.

185. Family Educational Rights and Privacy, 73 Fed. Reg. at 74,854.

186. FINAL REPORT, *supra* note 10, at 129–30; *see also* 34 C.F.R. § 99.36(a) (2019).

187. *When Is It Permissible To Utilize FERPA's Health or Safety Emergency Exception for Disclosures?*, U.S. DEP'T EDUC., https://studentprivacy.ed.gov/faq/when-it-permissible-utilize-ferpa's-health-or-safety-emergency-exception-disclosure [https://perma.cc/VRY2-BRZH].

188. *See* FINAL REPORT, *supra* note 10, at 131.

189. *Id.* at 132.

190. *See id.*

191. *Id.*

192. *See id.*

school's law enforcement unit for this purpose."[193] This will allow for the exposure of more student information to law enforcement and will make it more difficult to determine which individuals may gain access to FERPA-protected information and under which exception they may have a claim to that information. It seems that this would leave the door open for a school to overutilize this exception.

In 2018, the Department released a Frequently Asked Questions resource to clarify how photos and videos are protected under FERPA.[194] Arguably, this only complicated matters further. The FAQ stated that if responsibility for videos falls with the school's "law enforcement unit," the videos are not education records under FERPA and could be given to the police without consent or an exception.[195] However, if the videos *are* education records—which they presumably would be if they were not maintained by the school law enforcement unit—then there must be written consent, an applicable exception, or a judicial order before such records could be given to police.[196]

This explanation leaves much to be desired. Without a clearer standard, students will not know the extent to which video footage may be shared, particularly as it seems schools themselves struggle with understanding the rules.[197] The FAQ and the resulting confusion also have the potential to lead to more student encounters with the police. Student interactions with the police should remain as limited as possible in order to maintain the sanctity of the educational environment and avoid the variety of long-term negative consequences that can result from student encounters with law enforcement.

3. The "School Officials Exception" and Discretion

Another exception, the "school officials exception," allows "[e]ducational agencies and institutions [to] disclose [personally identifiable information] from education records without consent to school officials (including School Resource Officers), provided they meet the *school's* criteria for 'school officials' with 'legitimate educational interests.'"[198] This exception leaves a significant amount of discretion to the schools to determine who qualifies as a "school official." One consequence of the exception is that schools could designate School Resource Officers ("SROs") as school officials, thus creating a backdoor

193. *Id.*

194. Eric Barba, *Got a FERPA Request for Video? Consult the April 2018 FPCO Guidance Before Responding*, CONN. EDUC. L. BLOG (Aug. 28, 2018), https://www.connecticuteducationlawblog.com/2018/08/articles/ferpa/got-a-ferpa-request-for-video-consult-the-april-2018-fpco-guidance-before-responding/ [https://perma.cc/U5YY-XK8D]; *FAQs on Photos and Videos Under FERPA*, *supra* note 168.

195. *FAQs on Photos and Videos Under FERPA*, *supra* note 168.

196. *Id.*

197. *See* FINAL REPORT, *supra* note 10, at 131.

198. *Id.* at 130 (emphasis added); *see* 34 C.F.R. § 99.31(a)(1) (2019).

to the health and safety exception, which otherwise grants access to law enforcement officers in emergency situations only.

The Department's Privacy Technical Assistance Center issued a Q&A in February 2019 to shed some light on the relationship between law enforcement, SROs, and FERPA, and it revealed just how easily a school can make this designation.[199] If a law enforcement officer is an employee of the school and constitutes a "school official with a legitimate educational interest" according to the school's definition, the officer could then be considered a school official.[200] SROs and off-duty officers could also easily meet the requirements of being school officials simply by ensuring school safety, meeting the school's definition of school official, remaining subject to the use and redisclosure requirements of FERPA, and having a memorandum of understanding with the school.[201] The ease with which schools can allow law enforcement to access student information, even when it is limited to the purposes of promoting "school safety and the physical security of students,"[202] is extremely concerning with respect to the protection of students' rights. In addition to the risks associated with law enforcement interactions, as discussed in Part II, allowing SROs and other officers to act as school officials will further blur the line between police, who need probable cause to conduct a search, and school officials, who merely need reasonable suspicion. Thus, it will be easier for law enforcement to search students and consequently interfere with students' educational experiences.

The wide latitude the exception provides to schools to designate school officials, and therefore decide who has access to student records, may also create

199. *See* PRIVACY TECH. ASSISTANCE CTR., U.S. DEP'T OF EDUC., SCHOOL RESOURCE OFFICERS, SCHOOL LAW ENFORCEMENT UNITS, AND THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) 14 (Feb. 2019), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs_2-5-19_0.pdf [https://perma.cc/7Y59-EC8L].

200. *Id.* at 11 (internal quotation marks omitted).

201. SROs and off-duty officers may

> qualify as "school officials" under FERPA if they:
>
> 1. Perform an institutional service or function for which the school or district would otherwise use employees (*e.g.*, to ensure school safety);
>
> 2. Are under the "direct control" of the school or district with respect to the use and maintenance of the education records (*e.g.*, through a memorandum of understanding (MOU) that establishes data use restrictions and data protection requirements);
>
> 3. Are subject to FERPA's use and re-disclosure requirements in 34 CFR § 99.33(a), which provides that the PII from education records may be used only for the purposes for which the disclosure was made (e.g., to promote school safety and the physical security of students), and which limits the re-disclosure of PII from education records; and
>
> 4. Meet the criteria specified in the school or district's annual notification of FERPA rights for being school officials with legitimate educational interests in the education records.

Id. at 12.

202. *Id.*

inconsistent approaches under FERPA from school to school or even over time on a single campus, which could further confuse students and parents. While schools may have different discipline codes, all public schools are bound by the same federal law, so it follows normatively that a student should have the same legal protections regardless of which public school they attend. While it is important that schools have the autonomy to operate in the way that best meets the needs of their specific communities, the amount of discretion left to schools under this exception potentially allows schools to push the limits of FERPA and act in a way that is contrary to its intent. Students should have clarity as to whether their information will be protected and how their school's policies comport with the requirements. School autonomy should not come at the expense of student privacy.

An additional issue regarding the school officials exception is what, exactly, falls into the category of a "legitimate educational interest."[203] Schools must provide students with their own definitions of what constitutes a "legitimate educational interest."[204] The National Forum on Education Statistics ("NFES"), a subdivision of the Department of Education's National Center for Education Statistics, issued a guide to help education agencies understand their responsibilities to protect student information, including how to apply the school officials exception.[205] In the section of the guide entitled "Defining 'Legitimate Educational Interests,'" NFES fails to provide any precise definition of the term, suggesting only that schools "could make broad decisions based on legal requirements and good practices."[206] While the guide does include a brief sample policy for schools to use as a model, the NFES *guide* is not official departmental *guidance*, and thus it is possible that adherence to the model would not be sufficient to preclude a school from liability[207] for wrongly considering a specific situation to constitute a "legitimate educational

203. *See* 20 U.S.C. § 1232g(b)(1)(A) (2012 & Sup. IV 2016). A school official generally has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. U.S. DEP'T OF EDUC., THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT: GUIDANCE FOR ELIGIBLE STUDENTS 3 (Feb. 2011) [hereinafter U.S. DEP'T OF EDUC., FERPA GUIDANCE], https://www2.ed.gov/policy/gen/guid/fpco/ferpa/for-eligible-students.pdf [https://perma.cc/2U6V-2NEM].

204. U.S. DEP'T OF EDUC., FERPA GUIDANCE, *supra* note 203, at 3; *see* 34 C.F.R. § 99.31(a)(1)(i)(A) (2019).

205. NAT'L FORUM ON EDUC. STATISTICS, FORUM GUIDE TO PROTECTING THE PRIVACY OF STUDENT INFORMATION, at vii (Mar. 2004), https://nces.ed.gov/pubs2004/2004330.pdf [https://perma.cc/E99P-4BTY].

206. *Id.* at 51.

207. The Department of Education is the FERPA enforcement body and thus oversees compliance. An individual may file a complaint with the Department to hold their institution accountable. The Supreme Court held that there is no private right of action to enforce FERPA. Gonzaga Univ. v. Doe, 536 U.S. 273, 276 (2002).

interest."[208] The lack of clarity could open the door to school officials accessing sensitive information about students without actual legitimate reasons to do so.

Further, FERPA permits schools to consider even some third parties to be school officials under this exception if the party "[p]erforms an institutional service or function" otherwise performed by an employee, is "under the direct control" of the school "with respect to the use and maintenance of education records," and is subject to requirements concerning personally identifiable information.[209] This could be interpreted to include security companies that handle a wide range of student data, such as face images, fingerprints, location services, and attendance records. Even if third parties are prevented from selling data, there are risks of security breaches and violations of agreements.

The closest the Department of Education has come to addressing this third-party issue was in the context of education technology companies, which primarily support personalized learning platforms and other educational classroom software.[210] After one school required a parent to "accept the terms and conditions of its third-party online learning platforms in order to enroll her child," the Department found that the school had violated FERPA by impermissibly conditioning enrollment on a waiver of "the rights and protections accorded under FERPA."[211] This indicates there is some basis in the Department's own precedent for the argument that a school cannot force its students to allow biometric information to be uploaded into a system maintained by a third party. Nevertheless, the Department has failed to provide unequivocal guidance.

4. Concerns Regarding Applicability of FERPA to AI Surveillance

While the health and safety and school officials exceptions could be vital for security enhancements, in practice they make FERPA more malleable. Although the exceptions may occasionally be critical to prevent violence and self-harm, the Department has expanded FERPA to the point that it has opened some serious loopholes. Critics believe FERPA has been weakened to the point that it is practically useless and merely a protective cover for schools to avoid liability.[212] For instance, to consider all school surveillance video systems to be within the reach of law enforcement is to contradict the very purpose of

208. *See* NAT'L FORUM ON EDUC. STATISTICS, *supra* note 205, at 51.

209. 34 C.F.R. § 99.31(a)(1)(i)(B).

210. Lindsey Barrett & Amelia Vance, *Dept of Ed: Schools Cannot Require Parents or Students To Waive Their FERPA Rights Through Ed Tech Company's Terms of Service*, FERPA SHERPA (Jan. 20, 2018), https://ferpasherpa.org/ptac1/ [https://perma.cc/Q5RV-7DFR].

211. *Id.*

212. Greenberg, *supra* note 173; Schroeder, *supra* note 173.

FERPA. FERPA's original intent to protect the privacy of student records[213] is now at risk of being abandoned in the face of technologies that extract mass amounts of data from students.

In its December 2018 Final Report, the Department of Education's Federal Commission on School Safety called on Congress to collaborate in an effort to "modernize FERPA to account for changes in technology since its enactment" so that more advanced (and potentially more invasive) security technologies can be installed in schools for the purpose of reducing violence, including shootings.[214] Just as the courts have neglected to develop the law in keeping up with technological innovation, so has Congress. FERPA needs a new face—one that actually protects student privacy and clearly specifies when it is appropriate to step outside the confines of the law to prevent harm to students and others.

In fact, if strengthened, FERPA could supplement privacy protections beyond what the *T.L.O.* framework provides. The law could be amended to provide for explicit considerations regarding the private nature of information obtained through advanced technologies, specifying how the exceptions comport with technology and safety needs. There is a difference between personally identifiable information in the form of video or fingerprints and personally identifiable information in the form of attendance records. The former is inherently more personal and has the potential to expose the student to more negative consequences if released. Congress must consider and make explicit FERPA's applicability to surveillance data as schools implement AI technologies, particularly when the data (e.g., face images and fingerprint scans) is being stored in a system owned by an outside company. These systems are of heightened concern, particularly if they also surmise students' feelings, behaviors, and activities, as is the case with the "smart eye" technology discussed earlier.[215] As applied to threat assessment programs, an additional layer of concern exists around the safeguarding of data pertaining to students' mental health.[216] There is a delicate, complex balance between FERPA as a privacy protector and FERPA as a barrier to preventing school shootings. At the very least, to avoid compliance violations and liability under FERPA, students and guardians should be directly informed about what information AI companies are using in the name of security, how and where it is stored, and what is being done or could be done with the information.[217]

213. *See* 121 CONG. REC. 13,990 (1975) (remarks of Sen. Buckley); *FERPA*, ELECTRONIC PRIVACY INFO. CTR., *supra* note 176 ("FERPA protects the confidentiality of student educational records.").

214. FINAL REPORT, *supra* note 10, at 133.

215. *See supra* text accompanying notes 54–56.

216. *See* Stolzoff, *supra* note 57.

217. Members of Congress recently introduced a bill that would regulate facial recognition technology in commercial settings, but it does not address FERPA. *See* Commercial Facial Recognition

C. *State Laws*

While the federal government has been slow to act, states have taken it upon themselves to deal with student safety and security through state legislation. In 2018 alone, more than fifty state school safety bills were signed into law.[218] Since 2013, forty-one states have passed 126 laws that in some way address student privacy.[219] Many of the privacy laws address testing standards and data breach policies,[220] and some concern the relationship between student data and outside technology vendors.[221] However, only a handful of states have taken legislative action to limit the collection of biometric data in public schools.[222] Until the federal government begins to answer these questions, states should enact laws to ensure the protection of students' rights. In fact, a trend of state action may lead Congress to make changes.

1. Existing State Laws Regarding Biometrics in Schools

The few states that have acted to protect student biometric data have taken different approaches to the issue. In 2014, Florida completely banned[223] biometric data collection in public schools after state lawmakers cited the need for student privacy and protection.[224] The general sentiment by Florida lawmakers was that biometrics should not be used until there is more information about how it works and what will happen with the data.[225] Florida

Privacy Act of 2019, S. 847, 116th Cong. (2019) (proposing regulation of facial recognition technology in business without mentioning regulation in school settings); Press Release, Roy Blunt, U.S. Senator for Mo., Blunt, Schatz Introduce Bipartisan Commercial Facial Recognition Privacy Act (Mar. 14, 2019), https://www.blunt.senate.gov/news/press-releases/blunt-schatz-introduce-bipartisan-commercial-facial-recognition-privacy-act [perma.cc/7X4R-V6DB] (discussing the purpose of the proposed legislation).

218. *See supra* note 9 and accompanying text.

219. *State Student Privacy Laws*, FERPA SHERPA (Aug. 6, 2019), https://ferpasherpa.org/state-laws/ [https://perma.cc/DM3V-F3N6].

220. *Id.* (indicating, for example, that Arizona, California, Colorado, Connecticut, Indiana, Kansas, and Kentucky have laws addressing testing standards and data breaches).

221. *See, e.g.*, CAL. BUS. & PROF. CODE § 22584 (West 2017) (preventing K-12 technology service providers from disclosing much of the information they acquire); ME. REV. STAT. ANN. tit. 20-A, § 953 (Westlaw through 1st Spec. Sess. of 129th Leg.) (requiring technology operators to obtain explicit consent from parents or eligible students before using student data for a number of enumerated purposes); NEV. REV. STAT. ANN. § 388.272 (LexisNexis 2016) (mandating that schools include privacy and security provisions and penalties for noncompliance in contracts with data service providers).

222. ARIZ. REV. STAT. ANN. § 15-109 (2019); FLA. STAT. ANN. § 1002.222(1)(a) (West 2016); KAN. STAT. ANN. § 72-6315 (Westlaw through 2019 Reg. Sess.); LA. STAT. ANN. § 17:100.8(B) (2013).

223. FLA. STAT. ANN. § 1002.222(1)(a) ("An agency or institution . . . may not . . . [c]ollect, obtain, or retain information on the political affiliation, voting history, religious affiliation, or biometric information of a student or a parent or sibling of the student.").

224. Ujifusa, *Ramp Up Attention*, *supra* note 115.

225. *See* Ryan Kline, *Shedding Light on Florida's Biometric Ban*, SECUREIDNEWS (Sept. 29, 2014), https://www.secureidnews.com/news-item/shedding-light-on-floridas-biometric-ban/ [https://perma.cc/5T4D-YUAS].

state Senator Dorothy Hukill reasoned that "most people have no idea what the use of biometric information means, and even those who do understand it shouldn't have the choice to participate—for now."[226]

A handful of states—Illinois,[227] Louisiana,[228] Kansas,[229] and Arizona[230]—have passed laws that allow biometric collection in schools, but only if a parent or guardian consents. One such law was proposed in Missouri in January 2019 but has not made any progress.[231] Requiring guardians to give consent for certain types of information collection is a critical approach to managing biometrics in schools because it allows for autonomy and control over personal information.[232] This notice-and-consent requirement also aligns with the intent of FERPA to protect student privacy.[233]

2. State Responses to Biometric Use Generally

Only three states—Illinois,[234] Washington,[235] and Texas[236]—have laws that regulate the commercial use of biometric data. In Illinois, the Biometric Information Privacy Act "covers biometric information such as thumb prints or retinal images but also geometrical data gleaned from a person's face."[237] The Texas law closely resembles Illinois's law and also includes facial recognition, retina scans, and voice identification.[238] Meanwhile, Washington's law broadly defines biometric data but excludes specific types of imaging, suggesting that the law likely will not have a sufficient impact on the use of facial recognition technology.[239] San Francisco, however, is considering a ban on facial recognition

226. *Id.*

227. 105 ILL. COMP. STAT. ANN. 5/34-18.34(b)(1) (Westlaw through P.A. 101-115).

228. LA. STAT. ANN. § 17:100.8(B)(2) (2013).

229. KAN. STAT. ANN. § 72-6315 (Westlaw through 2019 Reg. Sess.).

230. ARIZ. REV. STAT. ANN. § 15-109 (2019).

231. *See* H.B. 783, 100th Gen. Assemb., 1st Reg. Sess. (Mo. 2019).

232. Wisconsin also considered a similar law. *See* Asemb. B. 616, 2013 Leg. (Wis. 2014). The Children's Online Privacy Protection Act ("COPPA") requires commercial websites and other online services to obtain parental consent before collecting information, including photographs and voice recordings, from children under the age of thirteen. 15 U.S.C. § 6502(b)(1)(A) (2012). COPPA provides a decent framework for how security companies in schools should approach data collection, but it only applies to certain types of service providers and thus does not fit squarely within the scope of this Comment. *See id*.

233. *See FERPA*, U.S. DEP'T EDUC., *supra* note 114.

234. 740 ILL. COMP. STAT. ANN. 14/10 to 14/15 (Westlaw through P.A. 101-115).

235. WASH. REV. CODE ANN. § 19.375.020 (Westlaw through 2019 Reg. Sess.).

236. TEX. BUS. & COM. CODE ANN. § 503.001 (Westlaw through the end of the 2019 Reg. Sess.).

237. Jeff John Roberts, *Judge Says Customers Can Sue Over Face Scans*, FORTUNE (Sept. 19, 2017), http://fortune.com/2017/09/19/shutterfly-face-scan/ [https://perma.cc/Z5WD-F4ZH]; *see* 740 ILL. COMP. STAT. ANN. 14/10 (Westlaw).

238. TEX. BUS. & COM. CODE ANN. § 503.001(a) (Westlaw).

239. *Washington Becomes the Third State with a Biometric Law*, COVINGTON: INSIDE PRIVACY (May 31, 2017), https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law/ [https://perma.cc/Q5RG-GUFT].

surveillance as well as audits of existing technologies in use, including ballistic detection.[240] The city's lawmakers proposed the ban due to concerns about privacy, machine bias, and misuse by law enforcement officials that could lead to an oppressive state.[241] These laws reflect a growing trend by states and municipalities to address privacy concerns surrounding biometric surveillance, which could serve as the impetus to expand protections to schools. Legislative action in the general surveillance field should inform how school surveillance is treated.

3. Potential for the Evolution of State Laws

For some, the appeal of advanced surveillance to reduce violence may be sufficient to suppress any concerns about privacy or societal impact. However, the move, albeit slow, toward bans or restrictions on collection of biometric data suggests a shift in the way the public and state lawmakers are thinking about these technologies. There is much left to learn about advanced surveillance technologies, but "[a]buse doesn't happen at the outset[, i]t happens when the technology becomes entrenched and dismantling it becomes unimaginable."[242] Thus, concerns need to be addressed at the beginning of the evolution, before it is too late. One school district in Texas, which does not regulate biometrics in schools, is already using the technology to track attendance in class and at school-sponsored social events and to process library book check-outs.[243] In Missouri, one school district is using biometric facial recognition cameras to identify individuals from law enforcement criminal databases, and the system can lock the school down when it identifies such an individual.[244]

These technologies are already ingrained in society and becoming normalized. One crucial issue is whether students in states without legal restrictions are able to opt out of surveillance programs. It is doubtful that students are truly given an option not to participate in school programs that

240. Gregory Barber, *San Francisco Could Be First To Ban Facial Recognition Tech*, WIRED (Jan. 31, 2019), https://www.wired.com/story/san-francisco-could-be-first-ban-facial-recognition-tech/ [https://perma.cc/V2R7-JR3C (dark archive)].

241. *Id.*

242. *Id.*; *see* Miller, *supra* note 43 (explaining the view that parents need to be educated about what the technologies are and how they will be used).

243. Shawna De La Rosa, *Biometrics Can Make Schools Safer, but Privacy Concerns Persist*, EDUC. DIVE (May 9, 2019), https://www.educationdive.com/news/biometrics-can-make-schools-safer-but-privacy-concerns-persist/554420/ [https://perma.cc/5AB6-MLFT]; Alana Hernandez, *Texas School District Purchases Biometric Scanning Technology*, GOV'T TECH. (Aug. 13, 2018), https://www.govtech.com/products/Texas-School-District-Purchases-Biometric-Scanning-Technology.html [https://perma.cc/N2TX-57SM].

244. Chris Burt, *Missouri School District Deploys Panasonic Facial Recognition for Security and Access Control*, BIOMETRIC UPDATE (Apr. 10, 2019), https://www.biometricupdate.com/201904/missouri-school-district-deploys-panasonic-facial-recognition-for-security-and-access-control [https://perma.cc/5796-TFTQ]; De La Rosa, *supra* note 243.

store their personal data, particularly when schools require the use of face scanners to open doors, geolocation programs to take attendance, or fingerprinting to pay for lunch. The development of Fourth Amendment jurisprudence moves slowly,[245] and it is unclear how the Supreme Court will treat advanced surveillance in schools. FERPA has many vague exceptions and loopholes, to the point that it is essentially toothless with respect to many facets of this issue.

As the most significant and efficient movement has been on the state level, it appears that state laws have the greatest potential for securing student privacy in the face of the growing use of biometrics and AI in schools. In addition to states' abilities to act more quickly than the Supreme Court and Congress, most regulation of K-12 schools comes at the state and local level. Thus, states are uniquely positioned to tailor their laws to the specific needs of their schools. States should ensure that schools are transparent with their students as to the types of information obtained, where and how it is stored, and if there is an option for students to opt out.

CONCLUSION

This Comment is not an argument against the implementation of lifesaving technologies in K-12 schools; the reality is that the AI surveillance technologies discussed in this Comment have not been proven to effectively save lives or prevent violence in schools. Furthermore, the black boxes and lack of intuition in AI programs, coupled with a lack of accountability by lawmakers and the U.S. Department of Education, prevent people from knowing exactly how these technologies are making decisions, which only increases the risk of pernicious behavior and due process concerns.[246] The risks to the academic environment and the long-term impacts of machine bias and privacy violations are sufficient reasons to pause the rapid acquisition of these technologies. Instead of emphasizing prevention and using mental health assessments and awareness programs, these technologies only respond to a crisis that already exists.

It is a critical time to discuss the problems, along with the excitement, that AI brings. The information available about the impact of AI surveillance in schools and how existing privacy laws apply to this type of surveillance is limited; students and guardians must have the necessary information and ability to make informed decisions. The United States Supreme Court has ruled that

245. Orin S. Kerr, *Fourth Amendment Remedies and Development of the Law: A Comment on* Camreta v. Greene *and* Davis v. United States, CATO SUP. CT. REV. 237, 237 (2011) ("The course of Fourth Amendment law slowly develops through the process of case-by-case adjudication.").

246. Tom Simonite, *AI Experts Want To End 'Black Box' Algorithms in Government*, WIRED (Oct. 18, 2017), https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/ [https://perma.cc/3KGB-XED6 (dark archive)].

Americans have the right to privacy and that this right extends to schools. It should not be so easy to compromise the societal value we have placed on individuals' rights.

More than anything, this must become an interdisciplinary conversation. Engineers should continue to develop AI surveillance technology to be maximally effective and accurate. Social scientists should research the impact of constant surveillance and potential false signals on children and young people. They should work together to eliminate bias in AI as well as determine the extent to which technologies like facial recognition work on younger, developing faces.[247] Lawyers should consider liability and keep elevating the conversation around due process concerns. Lawmakers should become more educated about the benefits and negative consequences of the technologies. In addition, educators, students, and parents should be involved in these conversations. There are already efforts to incorporate AI education into K-12 schools to ensure students have the knowledge necessary either to enter the field themselves or at least understand their roles and opinions in a world that is watching them.

At the very least, it is critical that the issues with AI are acknowledged. The impact that bias can have on students could be traumatic and long lasting. There has simply not been enough research into the potential risks of school surveillance technologies. It is the monetization of fear—doing whatever it takes to make people feel a little better, even if it does not work and puts education and student well-being at risk.

We are progressively normalizing the use of these technologies. When students go to school, they should feel safe. Nonetheless, we cannot turn the educational environment into schools of surveillance without doing proper reconnaissance first.

MAYA WEINSTEIN**

247. Schools should consider teaching their students software engineering and technology development. This would diversify the field and reduce the "bias in" during software development. *See supra* Section II.D.

** I would like to thank Professor Ann Klinefelter, Professor Jeff Ward, my Topic Editor Thomas Zamadics, and Jeanette Lee for all of their helpful guidance and inspiration. I am forever grateful to Scott Weinstein, Hetty Weinstein, and Andy MacCracken for their feedback and support during the writing process. My Primary Editor, Shannon Smith, and Executive Editor, Miranda Goot, as well as the Staff and Board Members who worked on this Comment, deserve significant praise for their time and commitment to strengthening this piece. Lastly, I would like to dedicate this piece to my grandfather, Alvin Weinstein, z"l, who taught me to think critically, write passionately, and advocate for justice.