AI Proctoring: Academic Integrity vs. Student Rights

SAMANTHA MITA[†]

Advancements in artificial intelligence ("AI") and machine learning have found their way into the classroom. The use of artificial intelligence proctoring services ("AIPS") has risen over the past few years with little consideration for the legal and ethical consequences of their implementation. Issues such as invasion of privacy and bias often get overlooked in favor of preconceived notions of fairness and infallibility associated with the concepts of AI and machine learning. These ethical concerns are especially magnified if AIPS are used in a K-12 setting. This Note, through a lens of AI ethics, recommends a two-pronged approach that creates an educational privacy right and provides concrete guidance for schools. Given that there are viable alternatives, AIPS should be implemented only after careful consideration, if at all.

[†] J.D. Candidate 2023, University of California College of the Law, San Francisco (formerly UC Hastings); Senior Articles Editor, *Hastings Law Journal*. My deepest gratitude for the support from my family and friends; guidance from my professor, Chimène Keitner; and the tireless efforts of the editors of the *Hastings Law Journal*.

TABLE OF CONTENTS

INTRODUCTION

Dana Jo read a question aloud on an online exam and received an academic infraction that put the scholarship she relied on to pay for food and rent at risk.[1] Why? Because the artificial intelligence ("AI") program administering the test flagged her behavior as suspicious.[2] Although Dana Jo ultimately convinced the school to expunge the infraction, it required her to contact school administration and the AI program vendor on her own.[3] Dana Jo's experience is not uncommon, and is a symptom of misguided confidence in technology to solve all problems.

The COVID-19 pandemic thrust remote education on unsuspecting students and schools around the world. As part of the remote learning toolbox, artificial intelligence proctoring services ("AIPS") were suddenly in high demand. Although AIPS adoption was a quick fix that helped schools continue to function, the hasty implementation left many questions regarding student rights like privacy, accessibility, and equity unanswered. In our race to replace human judgment with the veneer of technological neutrality and efficiency, we often forget that machines are fallible because they are made by people.

Part I of this Note presents a brief background on AI technology, the technologies currently in use, the reasons why AIPS have been adopted, and why AIPS will likely be adopted by the K-12 sector. Through a lens of AI ethics, Part II addresses the potential harms to students AIPS deployment in schools can cause. Part III delves into relevant federal student privacy laws and regulations, specifically the Family Educational Rights and Privacy Act of 1974 ("FERPA"),[4] the Children's Online Privacy Protection Act of 1998 ("COPPA"),[5] and the Federal Trade Commission's ("FTC") regulatory powers to demonstrate that these current laws do not effectively protect students from AI surveillance. Finally, Part IV argues that AIPS use should be paused until schools and governments are able to protect students from technological intrusions that undermine their basic rights to a fair and accessible education, and suggests a two-pronged approach to mitigate these harms.

1. Margot Harris, *A Student Says Test Proctoring AI Flagged Her as Cheating when She Read a Question Out Loud. Others Say the Software Could Have More Dire Consequences.*, BUS. INSIDER (Oct. 4, 2020, 6:30 AM), https://www.insider.com/viral-tiktok-student-fails-exam-after-ai-software-flags-cheating-2020-10.

2. *Id.*

3. *Id.*

4. Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

5. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

I. BACKGROUND ON AI & SCHOOL USAGE OF AIPS

A. WHAT IS AI?

Educational AI technology is estimated to be a $6 billion industry by 2024.[6] Yet despite this fact, the term "AI" does not have a commonly cited definition, most likely because what the technology encompasses has changed and continues to change over time.[7] The "father" of AI, Marvin Minsky, defined it as "the science of making machines do things that require intelligence if done by men."[8] In other words, "AI involves the study, design and building of intelligent agents that can achieve goals,"[9] where the "intelligent agent" is a machine programmed to think or act rationally like a human.[10] AI "learns" by looking at data in specific formats, with the inputs tagged so that the system can formulate observations that can then be used to understand other inputs without tags.[11]

Machine learning ("ML") is a subset of AI and is often used in products that allow a machine to make predictions without the input of humans.[12] ML focuses on training a computational model to accomplish a task or series of tasks using data.[13] In its most simplistic form, there are two kinds of ML—*supervised learning*, where a machine is fed a labeled training dataset in order to create a function based on the inputs, and *unsupervised learning*, which gives the machine *unlabeled* data, counting on an algorithm to create a function on its own based on similarities and trends that the algorithm finds.[14] Because ML is completely automated, tools that leverage this technology are scalable, efficient, and, in many cases, incredibly accurate.[15]

B. HOW ARE AI AND REMOTE PROCTORING SERVICES APPLIED IN SCHOOLS?

AI technology is currently used in several different educational applications, including personalized learning, tutoring, automating routine tasks

6. FENGCHUN MIAO, WAYNE HOLMES, RONGHUAI HUANG & HUI ZHANG, UNITED NATIONS EDUC., SCI. & CULTURAL ORG., AI AND EDUCATION: GUIDANCE FOR POLICY-MAKERS 5 (2021).

7. CHRISTOPH BARTNECK, CHRISTOPH LÜTGE, ALAN WAGNER & SEAN WELSH, AN INTRODUCTION TO ETHICS IN ROBOTICS AND AI 7–8 (2021).

8. MARVIN MINSKY, SEMANTIC INFORMATION PROCESSING v (1968).

9. BARTNECK ET AL., *supra* note 7, at 8.

10. *Id.*

11. *Id.* at 11.

12. *See* Simon Coghlan, Tim Miller & Jeannie Paterson, *Good Proctor or "Big Brother"? Ethics of Online Exam Supervision Technologies*, 34 PHIL. & TECH. 1581, 1585–86 (2021).

13. Daniel Martin Katz, *AI + Law*, *in* LEGAL INFORMATICS 87, 89 (Daniel Martin Katz et al. eds., 2021).

14. *Id.*

15. *See* Coghlan et al., *supra* note 12, at 1583.

like attendance-taking and grading, and testing.[16] Remote, online proctoring systems allow students to take tests in remote locations while still maintaining academic integrity.[17]

Remote proctoring is not new to academia, and is currently in use by many institutions, including for graduate admissions exams like the Graduate Record Examination ("GRE") and Graduate Management Admission Test ("GMAT").[18] There are generally three basic kinds of remote proctoring systems: live proctoring, recorded proctoring, and automated proctoring.[19] The first two heavily rely on human review.[20] In AIPS however, cheating and fraud are identified through various algorithms programmed into the system.[21] Since no humans are involved in this process, automated proctoring is easily scalable and much cheaper to implement.[22] AIPS are used for "test security" purposes by utilizing functionalities such as identity verification via biometrics, audio and video monitoring and recording, gaze tracking, and the ability to flag unwanted behavior.[23]

Due to impersonation concerns that arise from the online testing format, AIPS are often used for authenticating a test-taker's identity.[24] AIPS require each candidate to submit personal information or proof of identity before the test is launched in order to verify that the person taking the exam is truly the intended test-taker.[25] As laptops and mobile phones with voice, face, and fingerprint scanning capabilities become ubiquitous, biometric identification has proliferated.[26] In some advanced systems where the student is also attending class online, the software tracks and analyzes a student's unique behavior characteristics in class and provides that information to proctoring services in order to better monitor the observed behavior of the test-taker.[27]

Most AIPS leverage facial recognition technology ("FRT") to detect suspicious student activity, including looking for other people in a student's

16. JOYCE J. LU & LAURIE A. HARRIS, CONG. RSCH. SERV., IF10937, ARTIFICIAL INTELLIGENCE (A.I.) AND EDUCATION 1 (2018); Nathalie A. Smuha, Trustworthy Artificial Intelligence in Education: Pitfalls and Pathways 6 (Dec. 2020) (unpublished manuscript), https://ssrn.com/abstract=3742421.

17. Aditya Nigam, Rhitvik Pasricha, Tarishi Singh & Prathamesh Churi, *A Systematic Review on AI-Based Proctoring Systems: Past, Present and Future*, 26 EDUC. & INFO. TECHS. 6421, 6424–25 (2021).

18. *Id.* at 6424.

19. Mohammed Juned Hussein, Javed Yusuf, Arpana Sandhya Deb, Letila Fong & Som Naidu, *An Evaluation of Online Proctoring Tools*, 12 OPEN PRAXIS 509, 510 (2020).

20. *Id.*

21. *Id.*

22. *Id.*; Nigam et al., *supra* note 17, at 6440.

23. Nigam et al., *supra* note 17, at 6431–33.

24. *Id.* at 6440.

25. *Id.*

26. *Id.* at 6440–41.

27. *See, e.g.*, Ludwig Slusky, *Cybersecurity of Online Proctoring Systems*, 29 J. INT'L TECH. & INFO. MGMT. 56, 74 (2020) (describing the functionalities of the tool Examus).

room (a "multiple faces detected" flag).[28] By utilizing computer algorithms to match a person's face to a picture in a database—for example, matching a student's face to their school photo—FRT can be used as an identification verification method.[29] Other AI proctoring systems use gaze-detection algorithms or computer monitoring to flag "unusual" behavior from a test-taker.[30] For example, students can be flagged for anything from excessive head or eye movement, mouse clicks, typing cadence, excessive sound or talking, spotty internet, and other faces spotted in the background.[31] These systems typically require students to keep their cameras and microphones on, with some even requiring the student to provide a 360° scan of their room before the test will launch.[32] At the extreme end, there are options that automatically record the test-taker's screen the entire time,[33] use machines to track heartrate,[34] or require a "multimedia analytics system" involving a webcam, a "wearcam" (a camera that is clipped to the test-taker's clothing), and a microphone.[35] AIPS vendors have effectively leveraged advances in technology to create increasingly robust ways to monitor students.

C. WHY AI PROCTORING?

Educational institutions have adopted AIPS for several reasons. The most common goals are to prevent academic misconduct and protect exam integrity.[36] The American Council on Education endorses AIPS, acknowledging that "[w]hen you're educating thousands of students in an online setting, it's a good tool in the tool kit."[37] The COVID-19 pandemic required schools to pivot to remote learning with little notice—within a matter of weeks, and in some cases,

---

28. Drew Harwell, *Cheating-Detection Companies Made Millions During the Pandemic. Now, Students Are Fighting Back.*, WASH. POST (Nov. 12, 2020, 9:18 AM), https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/.

29. *Face Recognition*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/face-recognition (Oct. 24, 2017).

30. Harwell, *supra* note 28.

31. *Id.*

32. *Proctortrack Updates Mobile App with New Updates*, PROCTORTRACK, https://www.proctortrack.com/mobile-app/ (last visited May 12, 2023).

33. Nigam et al., *supra* note 17, at 6429.

34. Xuanchong Li, Kai-min Chang, Yueran Yuan & Alexander Hauptmann, *Massive Open Online Proctor: Protecting the Credibility of MOOCs Certificates*, *in* CSCW '15: PROCEEDINGS OF THE 18TH ACM CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK & SOCIAL COMPUTING 1129, 1130 (2015).

35. Yousef Atoum, Liping Chen, Alex X. Liu, Stephen D. H. Hsu & Xiaoming Liu, *Automated Online Exam Proctoring*, 19 IEEE TRANSACTIONS ON MULTIMEDIA 1609, 1609–24 (2017).

36. WILEY, ACADEMIC INTEGRITY IN THE AGE OF ONLINE LEARNING 5 (2020); Taylor Swaak, *A Vulnerability in Proctoring Software Should Worry Colleges, Experts Say*, THE CHRON. OF HIGHER EDUC., https://www.chronicle.com/article/a-vulnerability-in-proctoring-software-should-worry-colleges-experts-say (Jan. 7, 2022, 2:09 PM).

37. Shawn Hubler, *Keeping Online Testing Honest? Or an Orwellian Overreach?*, N.Y. TIMES (May 10, 2020), https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html.

days.[38] Online classes meant online testing in all fields for all grades, and schools looked to implement solutions to minimize disruptions and delays.[39]

Educators and students both want to have confidence that everyone is playing by the same rules and that those who break the rules will be held accountable. Students should feel invested in their education, and to do so, need to be secure in an environment where trying their best is enough—they should not have to worry about their peers getting ahead in "unethical ways."[40] AIPS allowed schools the flexibility to administer assessments to students wherever the students chose to be while maintaining academic integrity and stakeholder confidence in the exams.[41] Some studies show that students taking proctored online quizzes resulted in shorter quiz-taking times, lower scores, and less variation in performance across exams when compared to similar quizzes taken without AIPS use, implying that AIPS can increase exam integrity and compliance.[42]

Schools frequently point to accreditation requirements as the reason for implementing AIPS.[43] Accrediting institutions often require proof of summative, end-of-course exams for school accreditation, so providing assurance that the student receiving the grade is the one who completed the work is paramount.[44] Some vendors prey on these fears, touting that their tool is

38. Howard Blume, Hailey Branson-Potts, Ruben Vives & Alex Wigglesworth, *Millions Affected as Schools Across U.S Close To Combat Spread of Coronavirus*, L.A. TIMES (Mar. 14, 2020, 3:00 AM), https://www.latimes.com/california/story/2020-03-14/schools-close-coronavirus; *see Map: Coronavirus and School Closures in 2019–2020*, EDUC. WK., https://www.edweek.org/leadership/map-coronavirus-and-school-closures-in-2019-2020/2020/03 [https://web.archive.org/web/20210306220448/https://www.edweek.org/leadership/map-coronavirus-and-school-closures-in-2019-2020/2020/03].

39. Colleen Flaherty, *Big Proctor*, INSIDE HIGHER ED (May 11, 2020), https://www.insidehighered.com/news/2020/05/11/online-proctoring-surging-during-covid-19; David Matthews, *EU Lawmakers Call for Online Exam Proctoring Privacy Probe*, TIMES HIGHER EDUC. (May 5, 2020), https://www.timeshighereducation.com/news/eu-lawmakers-call-online-exam-proctoring-privacy-probe; *see also* Nigam et al., *supra* note 17, at 6422; Tyler Sonnemaker, *As Zoom Classes Take Over During the Pandemic, Edtech Companies Provide a Lifeline, but Only for Schools and Parents Willing To Surrender Their Students' Privacy*, BUS. INSIDER (Oct. 13, 2020, 1:37 PM), https://www.businessinsider.com/virtual-learning-privacy-tech-teachers-parents-schools-student-data-2020-10.

40. Julie Allegro Maples, *The Surveillance State of Education*, WHARTON MAG. (May 3, 2021), https://magazine.wharton.upenn.edu/digital/the-surveillance-state-of-education/.

41. Doug Lederman, *Best Way To Stop Cheating in Online Courses? 'Teach Better,'* INSIDE HIGHER ED (July 22, 2020), https://www.insidehighered.com/digital-learning/article/2020/07/22/technology-best-way-stop-online-cheating-no-experts-say-better; *Top 9 Remote Proctoring Benefits for Universities—and Their Students*, ROSALYN, https://www.rosalyn.ai/blog/top-9-remote-proctoring-benefits-for-universities-and-their-students (last visited May 12, 2023).

42. Helaine M. Alessio, Nancy Malay, Karsten Maurer, A. John Bailer & Beth Rubin, *Interaction of Proctoring and Student Major on Online Test Performance*, 19 INT'L. REV. RSCH. OPEN & DISTRIBUTED LEARNING 166, 166 (2018).

43. Kerryn Butler-Henderson & Joseph Crawford, *A Systematic Review of Online Examinations: A Pedagogical Innovation for Scalable Authentication and Integrity*, 159 COMPUTS. & EDUC. 8, 8 (2020).

44. *Id.*

necessary to assure accreditors that the school does indeed have the proper measures in place.[45] Moreover, some academics believe that the quality of the degree is directly dependent on the rigor of testing that went into earning it.[46] The CEO of Proctorio has asserted that without his company's anti-cheating services, future employers might not find a student's achievements "as credible," since schools will simply hand out "corona diploma[s]."[47] Similarly, some schools may falsely believe that surveillance solutions are necessary for compliance with state and federal laws.[48]

Both students and school staff can potentially benefit from the ancillary functionalities many AIPS offer. Educators have lauded the ease with which they can create, collect, and grade online exams,[49] freeing up time for more complex teaching activities[50] and returning results in some cases almost instantly.[51] AIPS provide simple scheduling since a live proctor is not required to administer the test,[52] encouraging accessibility to a diverse set of students.[53] This can also be beneficial to institutions that have a low teacher-to-student ratio[54] or communities that lack the resources to provide a high volume of monitoring.[55] From the student perspective, AIPS do not require them to endure taking their test while a live person watches them through a screen.[56] This could be perceived by some students as less "creepy,"[57] a common complaint of live-proctoring situations.[58] Additionally, in theory, AI systems can offer more transparency

45. Flaherty, *supra* note 39.

46. Nigam et al., *supra* note 17, at 6422.

47. Harwell, *supra* note 28.

48. Mark Keierleber, *Minneapolis School District Addresses Parent Outrage over New Digital Surveillance Tool as Students Learn Remotely*, THE 74 (Oct. 28, 2020), https://www.the74million.org/minneapolis-school-district-addresses-parent-outrage-over-new-digital-surveillance-tool-as-students-learn-remotely/ (explaining that online surveillance solutions like AIPS are not "actually required, mostly because we don't know what is required").

49. Butler-Henderson & Crawford, *supra* note 43.

50. *Id.*

51. Nigam et al., *supra* note 17, at 6440.

52. Tess Mitchell, *AI from a Proctor's Perspective*, HONORLOCK (Jan. 22, 2020), https://honorlock.com/blog/ai-from-a-proctors-perspective/; *see, e.g.*, *Top 9 Remote Proctoring Benefits for Universities—and Their Students*, *supra* note 41; Tyler Stike, *Top 10 Benefits of Online Proctoring*, HONORLOCK (June 14, 2021), https://honorlock.com/blog/top-10-benefits-of-online-proctoring/.

53. *Top 9 Remote Proctoring Benefits for Universities—and Their Students*, *supra* note 41.

54. Nigam et al., *supra* note 17, at 6422.

55. Filippo A. Raso, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz & Levin Kim, *Artificial Intelligence & Human Rights: Opportunities & Risks* 50 (Berkman Klein Ctr., Research Publication No. 2018-6, 2018), https://ssrn.com/abstract=3259344.

56. Monica Chin, *Exam Anxiety: How Remote Test-Proctoring Is Creeping Students Out*, THE VERGE (Apr. 29, 2020, 5:00 AM), https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education.

57. *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology*, *Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 60 (2013).

58. Chin, *supra* note 56.

than their human counterparts.[59] Machines cannot lie or hide bias, so it is possible that in some cases it may be easier to spot algorithmic bias in a machine's output than human bias if one is looking for it.[60] This could mean higher levels of accountability, earlier discovery, and quicker reduction of bias in systems.[61]

Economics and behavioral inertia have also likely contributed to schools' continued use of AIPS. For many schools, these services were not cheap or easy to implement,[62] so the schools cannot justify letting the system go after only a year of use.[63] Some AIPS contracts have been reported to be worth over half a million dollars for one year of service,[64] and schools have admitted to renewing these services simply because there were no better alternatives in place when the contract came up for renewal.[65] Given the volatility COVID-19 introduced to the daily operations of schools, many administrators and staff simply did not have the bandwidth to tackle issues like educational technology ("EdTech") evaluations in a timely way.[66]

D. ONLINE ASSESSMENTS & AIPS ARE COMING TO K-12

Thanks to advances in EdTech, "[t]he future of learning is digital."[67] Although the adoption of online learning was catalyzed by the COVID-19 pandemic, many believe that it will not end once the pandemic does.[68] The vendors that have secured thousands of contracts from the pandemic will want to hold on to their new clients and will continue to attempt to leverage those agreements into further services.[69] While AIPS are used primarily at the university level, many AIPS vendors do appear to be targeting K-12 schools,

---

59. Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation,"* 38 A.I. MAG. 50, 56 (2017).

60. Runshan Fu, Yan Huang & Param Vir Singh, AI and Algorithmic Bias: Source, Detection, Mitigation and Implications 24–25 (July 26, 2020) (unpublished manuscript), https://ssrn.com/abstract=3681517.

61. *Id.*

62. Swaak, *supra* note 36.

63. *See id.*

64. Harwell, *supra* note 28.

65. Swaak, *supra* note 36.

66. *Id.*

67. Mark Warschauer, *The Paradoxical Future of Digital Learning*, 1 LEARNING INQUIRY 41, 41 (2007).

68. Ong Ee Ing, *The Year of COVID-19: Personal Reflections on How Traditional Pedagogy Can Be Informed by Online Teaching Methods (aka How I Changed My Mind About Online Teaching)*, *in* LAW AND COVID-19 177, 183 (Aurelio Gurrea-Martínez et al. eds., 2020); Cathy Li & Farah Lalani, *The COVID-19 Pandemic Has Changed Education Forever. This Is How*, WORLD ECON. F. (Apr. 29, 2020), https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning/.

69. *See, e.g.*, Jeffrey R. Young, *Pushback Is Growing Against Automated Proctoring Services. But So Is Their Use*, EDSURGE (Nov. 13, 2020), https://www.edsurge.com/news/2020-11-13-pushback-is-growing-against-automated-proctoring-services-but-so-is-their-use (explaining Proctorio's partnership with McGraw-Hill to bundle its monitoring capabilities into courseware).

specifically advertising "K-12" services on their websites.[70] Furthermore, the use of AI is not foreign to K-12 institutions. Many have already adopted various AI surveillance systems for safety reasons.[71] Monitoring of student populations through on-campus cameras and microphones is already happening, as is AI software that monitors students' usage of social media.[72] Indeed, "students are . . . subjected to more forms of tracking . . . than ever before."[73] Lastly, as costs of infrastructure and operations continue to increase,[74] and as schools continue to struggle to hire educators,[75] schools may move toward more online learning, and therefore AIPS, to cope.

II. CONCERNS WITH AI PROCTORING

Nearly two-thirds of all colleges and universities in North America mention a proctoring system on their website, indicating widespread adoption of AIPS.[76] However, not everyone is happy with AIPS. Students have pushed back against AIPS, holding protests and signing petitions both in the United States and across the globe.[77] Their ire was sparked by the perceived invasion of privacy, anxiety the systems caused, concerns over the systems' ability to flag fairly, and an

70. *See, e.g.*, *Privacy Policy*, PROCTORIO, https://proctorio.com/privacy#inst-rep&us&all (Oct. 29, 2021); *Solutions for K-12*, RESPONDUS, https://web.respondus.com/k12/ (last visited May 12, 2023); *ProctorU Expands Online Proctoring of the G-Suite Certification Exam for K-12 Classrooms*, MEAZURE LEARNING (June 19, 2019), https://www.meazurelearning.com/resources/proctoru-expands-online-proctoring-of-the-g-suite-certification-for-k12-classrooms; *K-12*, PROCTORTRACK, https://www.proctortrack.com/k-12/ (last visited May 12, 2023); *Student Performance Insights for K-12*, EXAMSOFT, https://examsoft.com/programs/k-12/ (last visited May 12, 2023).

71. Amy B. Cyphert, *Tinker-ing with Machine Learning: The Legality and Consequences of Online Surveillance of Students*, 20 NEV. L.J. 457, 460 (2020).

72. *Id.* at 470.

73. *Id.* at 495.

74. Victoria Jackson & Nicholas Johnson, *America's School Infrastructure Needs a Major Investment of Federal Funds To Advance an Equitable Recovery*, CTR. ON BUDGET & POL'Y PRIORITIES (May 17, 2021), https://www.cbpp.org/research/state-budget-and-tax/americas-school-infrastructure-needs-a-major-investment-of-federal.

75. Cresencio Rodriguez-Delgado, Frances Kai-Hwa Wang, Gabrielle Hays & Roby Chavez, *Schools Across the Country Are Struggling To Find Staff. Here's Why*, PBS: NEWSHOUR (Nov. 23, 2021, 5:06 PM), https://www.pbs.org/newshour/education/schools-across-the-country-are-struggling-to-find-staff-heres-why; Kathryn Dill, *Teachers Are Quitting, and Companies Are Hot To Hire Them*, WALL ST. J. (Feb. 2, 2022, 7:26 AM), https://www.wsj.com/articles/teachers-are-quitting-and-companies-are-hot-to-hire-them-11643634181.

76. Royce Kimmons & George Veletsianos, *Proctoring Software in Higher Ed: Prevalence and Patterns*, EDUCAUSE REV. (Feb. 23, 2021), https://er.educause.edu/articles/2021/2/proctoring-software-in-higher-ed-prevalence-and-patterns.

77. Todd Feathers, *Schools Are Abandoning Invasive Proctoring Software After Student Backlash*, VICE (Feb. 26, 2021, 6:00 AM), https://www.vice.com/en/article/7k9ag4/schools-are-abandoning-invasive-proctoring-software-after-student-backlash; Avi Asher-Schapiro, *'Unfair Surveillance'? Online Exam Software Sparks Global Student Revolt*, REUTERS (Nov. 10, 2020, 4:25 AM), https://www.reuters.com/article/us-global-tech-education-feature-trfn/unfair-surveillance-online-exam-software-sparks-global-student-revolt-idUSKBN27Q1Q1.

overall distrust of both the AIPS system and their schools' ability to keep data secure.[78] Change.org has at least 173 petitions against the use of AIPS, with at least five different countries represented.[79] Moreover, students are not the only ones voicing their discontent. Faculty have also expressed their concerns,[80] and some universities have discouraged[81] or banned the use of AIPS altogether.[82] The uproar has caught the attention of both European and U.S. policymakers, resulting in both groups demanding more information and action from AIPS vendors.[83]

The potential for progress through AI is great, but as we become increasingly digitally interconnected, we must be conscientious of the impacts of the technology. In fact, current evaluations of AIPS have identified many concerns with this type of invigilation, and critics recommend that school

78. Drew Harwell, *Mass School Closures in the Wake of the Coronavirus Are Driving a New Wave of Student Surveillance*, WASH. POST (Apr. 1, 2020, 10:00 AM), https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/; Chin, *supra* note 56; Neil Selwyn et al., *A Necessary Evil? The Rise of Online Exam Proctoring in Australian Universities*, 186 MEDIA INT'L AUSTL. 2411, 2411–2502 (2021); Asher-Schapiro, *supra* note 77; Simon Coghlan, Jeannie Marie Paterson, Shaanan Cohney & Tim Miller, *Unis Are Using AI To Keep Students Sitting Exams Honest. But This Creates Its Own Problems*, THE CONVERSATION (Nov. 9, 2021, 1:21 PM), https://theconversation.com/unis-are-using-artificial-intelligence-to-keep-students-sitting-exams-honest-but-this-creates-its-own-problems-170708.

79. *Online Proctoring*, CHANGE.ORG, https://www.change.org/search?q=online+proctoring (last visited May 12, 2023).

80. *See, e.g.*, Eugene Volokh, *Can ProctorU Be Trusted with Students' Personal Data?*, REASON (Mar. 28, 2020, 8:59 AM), https://reason.com/volokh/2020/03/28/can-proctoru-be-trusted-with-students-personal-data/ (describing a professor's heated public exchange with a vendor over data mining concerns); Monica Chin, *An Ed-Tech Specialist Spoke Out About Remote Testing Software—and Now He's Being Sued*, THE VERGE (Oct. 22, 2020, 12:04 PM), https://www.theverge.com/2020/10/22/21526792/proctorio-online-test-proctoring-lawsuit-universities-students-coronavirus.

81. *See, e.g.*, Juliet E. Isselbacher & Amanda Y. Su, *Harvard Courses Turn to Monitored Exams, Open-Book Assessments, and Faith in Students as Classes Move Online*, HARV. CRIMSON (Mar. 27, 2020), https://www.thecrimson.com/article/2020/3/27/harvard-coronavirus-online-exams-academic-integrity/; Memorandum from Alison M. Wrynn, Assoc. V.C., Acad. Programs, Innovations & Fac. Dev., Cal. State Univ., to Provosts & Vice Presidents of Acad. Affs., Vice Presidents of Student Affs., Vice Presidents of Bus. & Fin. & Robert Keith Collins, Acad. Senate Chair, Cal. State Univ. 3 (Aug. 4, 2020), https://www.calstate.edu/impact-of-the-csu/technology/academic-technology-services/PublishingImages/Pages/alternative-instructional-modalities-and-resources/Online%20Proctoring%20Recommendations%20to%20Provosts,%20July%202020.pdf [hereinafter Wrynn Memorandum].

82. *See, e.g.*, Feathers, *supra* note 77; Olivia Buccieri, *Online Exam Proctoring No Longer Allowed for UC Berkeley Classes*, THE DAILY CALIFORNIAN (Apr. 5, 2020), https://www.dailycal.org/2020/04/05/online-exam-proctoring-no-longer-allowed-for-uc-berkeley-classes/; Memorandum from the Working Grp. on Online Examinations and Proctoring for the Spring Semester, Univ. of Cal., Berkeley (Apr. 20, 2020), https://academic-senate.berkeley.edu/sites/default/files/guidance_and_recommendations_from_the_working_group_on_exams_and_proctoring.pdf [hereinafter Berkeley Memorandum].

83. Matthews, *supra* note 39; *Blumenthal Leads Call for Virtual Exam Software Companies To Improve Equity, Accessibility & Privacy for Students amid Troubling Reports*, RICHARD BLUMENTHAL (Dec. 3, 2020), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-leads-call-for-virtual-exam-software-companies-to-improve-equity-accessibility-and-privacy-for-students-amid-troubling-reports.

administrators minimize their use of surveillance technology altogether.[84] Participants at the United Nations' Online Expert Seminar on Artificial Intelligence and the Right to Privacy even went so far as recommending the "banning of certain AI technologies, such as facial recognition . . . in schools."[85] Educational institutions have the responsibility to have the right systems in place to fully comprehend, and be held accountable for, their EdTech decisions.[86]

A lens of AI ethics can help mitigate these concerns.[87] Scholars and industry leaders from different backgrounds and philosophies have all consistently identified the following as core principles: (1) fairness, robustness, and bias; (2) accessibility, efficacy, and performance; (3) accountability and transparency; (4) privacy; (5) respect for autonomy; and (6) data security.[88] Therefore, these principles serve as a guiding framework. This Note will evaluate only two to four of the main concerns each principle raises for brevity's sake.

---

84. Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. REV. 1673, 1722 (2019).

85. OFF. OF THE UNITED NATIONS HIGH COMM'R FOR HUM. RTS., REPORT OF THE PROCEEDINGS OF THE ONLINE EXPERT SEMINAR WITH THE PURPOSE OF IDENTIFYING HOW AI, INCLUDING PROFILING, AUTOMATED DECISION-MAKING AND MACHINE LEARNING TECHNOLOGIES MAY, WITHOUT PROPER SAFEGUARDS, AFFECT THE ENJOYMENT OF THE RIGHT TO PRIVACY 14 (2020), https://www.ohchr.org/Documents/Issues/DigitalAge/ExpertSeminarReport-Right-Privacy.pdf.

86. Coghlan et al., *supra* note 12, at 1600.

87. DAVID LESLIE, THE ALAN TURING INST., UNDERSTANDING ARTIFICIAL INTELLIGENCE ETHICS AND SAFETY: A GUIDE FOR THE RESPONSIBLE DESIGN AND IMPLEMENTATION OF AI SYSTEMS IN THE PUBLIC SECTOR 3 (2020), https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf.

88. *See, e.g.*, Coghlan et al., *supra* note 12, at 1586–92 (describing principles of fairness, non-maleficence, transparency, privacy, accountability, and respect for autonomy); Kevin Buehler, Rachel Dooley, Liz Grennan & Alex Singla, *Getting To Know—and Manage—Your Biggest AI Risks*, MCKINSEY & CO. (May 3, 2021), https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/getting-to-know-and-manage-your-biggest-ai-risks (describing AI risks arising around privacy, data security, fairness, transparency and explainability, safety and performance, and third-party concerns); Smuha, *supra* note 16, at 5 (describing the requirements for trustworthy AI to be respect for human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, nondiscrimination and fairness, societal and environmental wellbeing, and accountability); Liane Colonna, *Legal Implications of Using AI as an Exam Invigilator* 10 (Stockholm Univ., Research Paper No. 91, 2021) (describing the European Union's High-Level Expert Group on AI's Ethics Guidelines on AI as including human agency and oversight; robustness and safety; privacy and data governance; transparency; diversity, nondiscrimination, and fairness; societal and environmental well-being; and accountability); *Universal Guidelines for Artificial Intelligence*, PUB. VOICE (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/; Valerie Strauss, *Why a "Student Privacy Bill of Rights" Is Desperately Needed*, WASH. POST (Mar. 6, 2014, 3:30 PM), https://www.washingtonpost.com/news/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed; ORGANISATION FOR ECON. CO-OPERATION & DEV., RECOMMENDATION OF THE COUNCIL ON ARTIFICAL INTELLIGENCE 7–8 (2019) (describing human-centered values, or fairness, transparency or explainability; security or safety; and accountability as key principles for AI actors); Anna Jobin, Marcello Ienca & Effy Vayena, *Artificial Intelligence: The Global Landscape of Ethics Guidelines*, 1 NATURE MACH. INTEL. 389, 395 (2019) (describing transparency, justice and fairness, non-maleficence, responsibility, privacy, beneficence, freedom and autonomy, trust, dignity, sustainability, and solidarity as key principles of AI ethics).

A. FAIRNESS, ROBUSTNESS & BIAS

Machines are commonly assumed to be more objective than humans, appearing to be neutral observers, which provides a sense of trust and reliability in their decisionmaking.[89] In reality, however, the algorithms used by machines are created by humans, and humans are imperfect and can infect the algorithms they create with their biases.[90] Critics of AI surveillance point to research that has consistently shown that FRT systems struggle to accurately identify the faces of nonwhite nonmales.[91] Critics do not argue that this inconsistency in performance was created intentionally, but rather that it is the result of a relatively homogenous set of programmers who created software based on their own life experiences and that it simply reflects the entrenched biases and discriminatory patterns that permeate society.[92] Regardless of intent, the adverse consequences of biased AI decisionmaking cannot be ignored. Because of the perceived veil of neutrality, AI systems can mask existing inequities, allowing new inequities to grow.[93] A 2022 Pew Research Center survey found that less than half of Americans think police use of FRT to find a person who may have committed a crime is a good idea for society.[94] In response to these studies, the

89. Cyphert, *supra* note 71, at 473.

90. *Id.* at 473–74; Fu et al., *supra* note 60, at 18–21.

91. *See* Joy Buolamwini, *Gender Shades*, MIT MEDIA LAB, https://www.media.mit.edu/projects/gender-shades/overview/ (last visited May 12, 2023); Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/; Chad Boutin, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. OF STANDARDS & TECH. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; Associated Press Staff, *Amazon Face-Detection Technology Shows Gender and Racial Bias, Researchers Say*, CBS NEWS (Jan. 25, 2019, 8:25 PM), https://www.cbsnews.com/news/amazon-face-detection-technology-shows-gender-racial-bias-researchers-say/; *see also* STAN. UNIV. HUM.-CENTERED A.I., THE AI INDEX 2022 ANNUAL REPORT 11 (2022), https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf (describing how, as AI language models grow "more capable over time[,] . . . so does the potential severity of their biases").

92. *See* Jonathan Vanian, *Eye on A.I.—How To Fix Artificial Intelligence's Diversity Crisis*, FORTUNE (Apr. 23, 2019, 1:52 PM), https://fortune.com/2019/04/23/artificial-intelligence-diversity-crisis/; Cyphert, *supra* note 71, at 462–64; Kari Paul, *'Disastrous' Lack of Diversity in AI Industry Perpetuates Bias, Study Finds*, THE GUARDIAN (Apr. 16, 2019, 8:47 PM), https://www.theguardian.com/technology/2019/apr/16/artificial-intelligence-lack-diversity-new-york-university-study; Alex Woodie, *Data Science and AI Predictions for 2022*, DATANAMI (Jan. 3, 2022), https://www.datanami.com/2022/01/03/data-science-and-ai-predictions-for-2022/; *Bias, Racism and Lies: Facing Up to the Unwanted Consequences of AI*, UN NEWS (Dec. 30, 2020), https://news.un.org/en/story/2020/12/1080192.

93. Lindsey Barrett, *Rejecting Test Surveillance in Higher Education*, 2022 MICH. ST. L. REV. 675, 723.

94. Lee Rainie, Cary Funk, Monica Anderson & Alec Tyson, *AI and Human Enhancement: Americans' Openness Is Tempered by a Range of Concerns*, PEW RSCH. CTR. (Mar. 17, 2022), https://www.pewresearch.org/internet/2022/03/17/ai-and-human-enhancement-americans-openness-is-tempered-by-a-range-of-concerns.

desire to avoid unequal outcomes, and public outcry, many cities have either established a moratorium on or banned FRT use completely.[95]

The use of AIPS and FRT in schools also has the potential to exacerbate existing biases. Unsurprisingly, at the input stage, students report that AIPS frequently flag innocent activity during exams, with students of color, students with disabilities, and students who wear religious garb experiencing a disproportionate number of flags,[96] potentially leading to unnecessary negative interactions with school officials or even law enforcement.[97] Like Dana Jo, students who receive too many flags are often sent to an academic board for review, and, depending on school policy, may receive a failed grade on their transcript until the issue is resolved.[98] This can take months, costing a student valuable opportunities due to the stigma associated with the disciplinary review, or simply a lower GPA.[99] Creating an environment rife with suspicion may cause students of color to drop out, thereby impacting their economic power, physical health, and future success.[100] Furthermore, this can perpetuate the "school-to-prison pipeline"[101] because students who face disproportionate disciplinary actions in K-12 have an increased risk of entering the criminal justice system.[102] Because police are more likely to use force on people of color, administrative and disciplinary actions can easily lead to even greater physical harms.[103]

The possibility for bias also exists at the output stage, where the interpretation of the algorithm's results is influenced by the educator's personal biases.[104] This interpretation is problematic because the reviewer lacks transparency into how the system determines what to flag, making it challenging for a reviewer to make a fully informed and unbiased decision.[105] Worse still, schools could use the flag as a pretext for accusations of cheating based on instructor biases. For example, education researchers have found that high-

95. *See, e.g.*, S.F., CAL., ADMIN. CODE § 19B (2019); PORTLAND, OR., CITY CODE ch. 34.10 (2020); BOSTON, MASS., MUN. CODE §§ 16-62 to -63 (2021); *see also Facial Recognition Laws in the United States #ProjectPanoptic*, INTERNET FREEDOM FOUND. (May 3, 2021), https://internetfreedom.in/facial-recognition-laws-in-the-united-states-projectpanoptic/.

96. Maples, *supra* note 40.

97. Maya Weinstein, *School Surveillance: The Students' Rights Implications of Artifical Intelligence as K-12 Public School Security*, 98 N.C. L. REV. 438, 455 (2020).

98. *Id.* at 457.

99. *Id.*; Cyphert, *supra* note 71, at 471.

100. Weinstein, *supra* note 97, at 456; AM. PUB. HEALTH ASS'N, THE DROPOUT CRISIS: A PUBLIC HEALTH PROBLEM AND THE ROLE OF SCHOOL-BASED HEALTH CARE 3 (2018), https://www.apha.org/-/media/files/pdf/sbhc/dropout_crisis.

101. ABA, ABA TASK FORCE ON REVERSING THE SCHOOL-TO-PRISON PIPELINE 8 (2018), https://www.americanbar.org/content/dam/aba/administrative/crsj/webinar/october-2021/aba-task-force-on-reversing-the-school-to-prison-pipeline-report.pdf.

102. Weinstein, *supra* note 97, at 456.

103. *Id.* at 455.

104. Cyphert, *supra* note 71, at 478.

105. *Id.*

achieving black male students are often accused of cheating due to their professors' assumptions that they could not have possibly performed as well as they had.[106] And even if the instructor was not biased, simply being flagged could impact the way the instructor perceives and interacts with those students,[107] creating a tendency for bias. Research has shown that online standardized exams already hurt vulnerable students'[108] test scores the most.[109] It is unreasonable to put yet another finger on the scale against vulnerable students' success.

Although AIPS vendors have considered the criticism and attempted to revamp their products with improved technology, students remain distrustful.[110] As librarian, researcher, and outspoken AIPS critic Shea Swauger puts it, "[d]o you care more about some students who will experience discrimination or some students who might cheat?"[111]

B. ACCESSIBILITY, EFFICACY & PERFORMANCE

All students deserve access to education and an environment where learning is the goal, not suspicion and mistreatment. According to an Educause poll of peer and industry experts, more than a third of respondents were concerned about a proctoring product's efficacy and accessibility.[112] Not all students have access to the technology online tests require, especially those who are already members of vulnerable populations.[113] Remote exams often require students to have their own personal device for test-taking, and consistent access

106. Shaun R. Harper & Charles H.F. Davis III, *Eight Actions To Reduce Racism in College Classrooms*, AAUP, https://www.aaup.org/article/eight-actions-reduce-racism-college-classrooms#.YIwoBWZJHzc (last visited May 12, 2023).

107. Lindsay McKenzie, *Time To Rethink AI Proctoring?*, INSIDE HIGHER ED (May 28, 2021), https://www.insidehighered.com/news/2021/05/28/are-colleges-checking-ais-work-remote-exam-proctoring.

108. "Vulnerable students" means those from low-income families, those who have disabilities, and those who are English language learners.

109. *See, e.g.*, Youki Terada, *On Standardized Tests, Students Face an 'Online Penalty*,*'* EDUTOPIA (July 8, 2020), https://www.edutopia.org/article/standardized-tests-students-face-online-penalty; Ben Backes & James Cowan, *Is the Pen Mightier Than the Keyboard? The Effect of Online Testing on Measured Student Achievement*, 68 ECON. EDUC. REV. 89, 90 (2019).

110. Katie Deighton, *Online Proctoring Programs Try To Ease the Tensions of Remote Testing*, WALL ST. J. (Apr. 13, 2021, 5:00 AM), https://www.wsj.com/articles/online-proctoring-programs-try-to-ease-the-tensions-of-remote-testing-11618304400.

111. Shea Swauger, *Remote Testing Monitored by AI Is Failing the Students Forced To Undergo It*, NBC NEWS (Nov. 7, 2020, 1:30 AM), https://www.nbcnews.com/think/opinion/remote-testing-monitored-ai-failing-students-forced-undergo-it-ncna1246769.

112. Susan Grajek, *COVID-19 QuickPoll Results: Grading and Proctoring*, EDUCAUSE REV. (Apr. 10, 2020), https://er.educause.edu/blogs/2020/4/educause-covid-19-quickpoll-results-grading-and-proctoring.

113. Lucie Cerna, Alexandre Rutigliano & Cecilia Mezzanotte, *The Impact of COVID-19 on Student Equity and Inclusion: Supporting Vulnerable Students During School Closures and School Re-Openings*, OECD (Nov. 19, 2020), https://www.oecd.org/coronavirus/policy-responses/the-impact-of-covid-19-on-student-equity-and-inclusion-supporting-vulnerable-students-during-school-closures-and-school-re-openings-d593b5c8/.

to the internet is crucial for any sort of remote proctoring to function.[114] In the spring of 2020, a survey done by the Consortium for School Networking found that many under-resourced districts did not have the digital integration or the resources to get students the devices or internet access required for remote learning.[115] And even those districts that did report having a device for every student still found that many of their students did not have the bandwidth necessary to support streaming video.[116] Students without consistent and reliable access to the necessary technologies and environment are at a disadvantage since they cannot meet the technical requirements AIPS impose and may therefore be precluded from taking particular classes. The loss of educational opportunities for marginalized students is problematic, as is the resulting increased homogeneity in the classroom.[117] Requiring AIPS for all students encourages technological ableism and exacerbates the "digital divide."[118]

For AIPS to be accessible, they need to account for the myriad of ways students "move, learn, process information, and demonstrate knowledge."[119] AIPS functionalities like gaze tracking are cognitively biased and may harm neurodivergent students or those with other disabilities by flagging students' disability-specific behavior as suspicious.[120] AIPS "presume[] that there is one normal kind of body and one normal kind of learning."[121] AIPS put up barriers to students who may struggle with ADHD and need to pace around the room, students who have motor tics due to cerebral palsy or Tourette's, students with dyslexia who need to verbalize questions, blind students who need screen readers or have atypical eye movements, and autistic students who may act in "unpredictable" ways.[122] The disparate impact on those students with disabilities

114. Mark Lieberman, *Many Districts Won't Be Ready for Remote Learning If Coronavirus Closes Schools*, EDUC. WK. (Mar. 5, 2020), https://www.edweek.org/leadership/many-districts-wont-be-ready-for-remote-learning-if-coronavirus-closes-schools/2020/03; Nigam et al., *supra* note 17, at 6435.

115. Lieberman, *supra* note 114; Sarah D. Sparks, *Remote Learning Isn't Just for Emergencies*, EDUC. WK. (Sept. 14, 2021), https://www.edweek.org/technology/remote-learning-isnt-just-for-emergencies/2021/09.

116. *Id.*

117. Barrett, *supra* note 93, at 730.

118. *See generally* SUMIT CHANDRA, AMY CHANG, LAUREN DAY, AMINA FAZLULLAH, JACK LIU, LANE MCBRIDE, THISAL MUDALIGE & DANNY WEISS, COMMON SENSE MEDIA & BOS. CONSULTING GRP., CLOSING THE K–12 DIGITAL DIVIDE IN THE AGE OF DISTANCE LEARNING (2020), https://www.commonsensemedia.org/sites/default/files/research/report/common_sense_media_report_final_7_1_3pm_web.pdf (providing further details on what the "digital divide" is and how it impacts remote learning).

119. Lydia X.Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, CTR. FOR DEMOCRACY & TECH. (Nov. 16, 2020), https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students.

120. Thomas Claburn, *Using 'AI-Based Software Like Proctorio and ProctorU' To Monitor Online Exams Is a Really Bad Idea, Says Uni Panel*, THE REG. (Aug. 20, 2021, 11:30 PM), https://www.theregister.com/2021/08/20/ai_proctoring_software/; Brown, *supra* note 119.

121. Brown, *supra* note 119.

122. *Id.*

compared to those without could potentially leave schools open to liability.[123] Moreover, students should not have to disclose any of the above conditions to their school if they do not wish to. Imposing AIPS could compel students to do just that, violating their privacy.

Additionally, there is evidence that FRTs can give false positive results more often for young faces.[124] There is also no evidence that FRTs are accurately able to identify or recognize developing faces.[125] A student's appearance can change greatly over the course of a school year, especially during puberty.[126] Putting aside biology, critics argue that this is an especially significant concern for preteen and teenage students who may change their appearance daily as they explore their identities and experiment with different ways of expressing themselves.[127] Transgender and nonbinary students may also run into even more difficulties, or even be outed because of discrepancies in their names or particular gender expression that day.[128]

Perhaps most importantly, there is limited evidence that the use of AIPS reduces cheating behaviors—schools may simply be wasting their limited resources on "security theater."[129] At the University of Texas at Austin, a 2021 report found that less than half of the twenty-seven cases that were referred to the Student Conduct and Academic Integrity Office were upheld.[130] Moreover, as discussed in this Part, from a pedagogical perspective, AIPS do not improve student outcomes and are in fact counterproductive to a healthy learning environment. Students report large amounts of anxiety over being watched, which reduces their cognitive capacity as their nervousness directs their energy elsewhere.[131] Psychologically, some students lose their belief in themselves

123. Swauger, *supra* note 111.

124. *See generally Facial Recognition Technology (FRT) Testimony: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. (2020) (statement of Charles H. Romine, Dir., Info. Tech. Lab'y, Nat'l Inst. of Standards & Tech., U.S. Dep't of Com.).

125. Weinstein, *supra* note 97, at 457.

126. K. Suzanne Scherf, Marlene Behrmann & Ronald E. Dahl, *Facing Changes and Changing Faces in Adolescence: A New Model for Investigating Adolescent-Specific Interactions Between Pubertal, Brain and Behavioral Development*, 2 DEV. COGNITIVE NEUROSCI. 199, 206 (2012).

127. Weinstein, *supra* note 97, at 457.

128. Swauger, *supra* note 111; Nora Caplan-Bricker, *Is Online Test-Monitoring Here To Stay?*, THE NEW YORKER (May 27, 2021), https://www.newyorker.com/tech/annals-of-technology/is-online-test-monitoring-here-to-stay; Harris, *supra* note 1.

129. Swaak, *supra* note 36; Butler-Henderson & Crawford, *supra* note 43, at 6; Rebecca Heilweil, *Paranoia About Cheating Is Making Online Education Terrible for Everyone*, VOX (May 4, 2020, 7:00 AM), https://www.vox.com/recode/2020/5/4/21241062/schools-cheating-proctorio-artificial-intelligence.

130. Claburn, *supra* note 120.

131. Anushka Patil & Jonah Engel Bromwich, *How It Feels when Software Watches You Take Tests*, N.Y. TIMES (Sept. 29, 2020), https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html; Darrell M. West, *TechTank Podcast Episode 23: How Should Universities Deal with Student Cheating?*, BROOKINGS, at 10:35 (July 12, 2021), https://www.brookings.edu/blog/techtank/2021/07/12/techtank-podcast-episode-23-how-

because they are told preemptively that the school does not think they can do the work fairly.[132] Such students lose the motivation to learn since the experience is so unpleasant, and are subsequently able to rationalize their dishonest behavior since the school expected them to cheat anyway.[133] Some critics claim that by implementing AIPS, schools are just paying a lot to harm children and "undermine all of those feelings of respect, trust, and community that we've found to be so effective in helping students to do what they understand to be the right thing."[134]

C. ACCOUNTABILITY & TRANSPARENCY

Instead of responding to critiques of bias or unfairness directly, AIPS vendors often fail to take responsibility and obfuscate accountability arguments by pointing out the convenience of their services.[135] Vendors clarify that "AI is an information gathering and assessment engine," and should be treated like "a smoke detector alerting humans to a possible problem" where the human educators make the call, not the technology.[136] They point out that a typical AIPS monitoring service costs the school twenty-five cents per session, while a live in-person proctor might cost the school twenty-five dollars or more, evidence that the services rendered must surely be different.[137] However, critics insist that many professors do not understand that AI is fallible and will simply act on reports without reviewing them,[138] analogous to how judges relied on sentencing guidelines provided by an algorithm.[139] To address this, some AIPS vendors will have staff members review the flagged footage to take the onus off faculty, but this is not the norm.[140]

---

should-universities-deal-with-student-cheating/; Nigam et al., *supra* note 17, at 6436; *Privacy for Students*, ELEC. FRONTIER FOUND. (Mar. 1, 2020), https://ssd.eff.org/en/module/privacy-students.

132. Mark Lieberman, *Exam Proctoring for Online Students Hasn't Yet Transformed*, INSIDE HIGHER ED (Oct. 10, 2018), https://www.insidehighered.com/digital-learning/article/2018/10/10/online-students-experience-wide-range-proctoring-situations-tech.

133. West, *supra* note 131.

134. *Id.* at 22:20.

135. McKenzie, *supra* note 107; *see, e.g.*, Ashley Norris, *What AI Really Does Not Do During an Online Test*, ELEARNING INDUS. (Jan. 18, 2021), https://elearningindustry.com/what-ai-really-does-not-do-during-online-test.

136. Norris, *supra* note 135.

137. McKenzie, *supra* note 107.

138. *Id.*

139. Ellora Thadaney Israni, *When an Algorithm Helps Send You to Prison*, N.Y. TIMES (Oct. 26, 2017), https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html; Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; *see also* Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1121 (2017).

140. McKenzie, *supra* note 107.

Vendors spend a lot of money developing their systems and rely on trade secret protections to avoid disclosing any actionable information about how their proprietary algorithms work.[141] In some cases, even if a vendor was open to or directed to share their algorithm, they might not be able to explain how it works because it was created by ML rather than coded by the vendors' engineers.[142] In these cases, the only way to tease out potential discrimination is to analyze outcomes, which can be difficult to access since the data is likely confidential and belongs to the vendor.[143] Moreover, algorithmic decisionmaking complicates Title VII disparate treatment and impact analyses because intent can be difficult to explicate from evidence of how an algorithm works.[144] Regardless, even if a complainant had access to the data, having enough to be statistically significant to prove either a disparate impact or disparate treatment claim is unlikely.

D. PRIVACY

Many studies have concluded that there are significant privacy gaps with AIPS.[145] In a 2020 summer survey of 1,200 parents, the Center for Democracy and Technology found that although "solid majorities believe[d] technology is 'worth the risk' to deliver key education benefits," this did not include AIPS.[146] Many students and parents felt that the requirement was "an Orwellian [o]verreach"[147] and that the cost of public school attendance was student privacy.[148] An infamous example of this is Proctorio's CEO's inappropriate posting of a student's support logs on Reddit.[149] The student had complained about his poor user experience, and the CEO, in addition to publicly posting the support logs, tried to shame him with the comment: "If you're gonna lie

141. *See* Jessica M. Meyers, *Artificial Intelligence and Trade Secrets*, AM. BAR ASS'N (Feb. 19, 2019), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/january-february/artificial-intelligence-trade-secrets-webinar; Fu et al., *supra* note 60, at 15.

142. Fu et al., *supra* note 60, at 15.

143. *Id.*

144. Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, *Accountable Algorithms*, 165 U. PA. L. REV. 633, 693 (2017) (describing disparate treatment as when the law recognizes liability for formal application of different procedures for different groups, or where there is an intent to discriminate, and disparate impact as when the law places liability on entities for different outcomes for different classes, regardless of intent).

145. *See* Nigam et al., *supra* note 17, at 6442.

146. Sonnemaker, *supra* note 39.

147. Wrynn Memorandum, *supra* note 81, at 2.

148. Sonnemaker, *supra* note 39.

149. Naaman Zhou, *CEO of Exam Monitoring Software Proctorio Apologises for Posting Student's Chat Logs on Reddit*, THE GUARDIAN (July 1, 2020, 2:27 PM), https://www.theguardian.com/australia-news/2020/jul/01/ceo-of-exam-monitoring-software-proctorio-apologises-for-posting-students-chat-logs-on-reddit; Complaint of EPIC at 9, *In re* Online Test Proctoring Cos., Off. of the Att'y Gen. of D.C. (Dec. 9, 2020), https://epic.org/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf [hereinafter EPIC Complaint].

bro . . . don't do it when the company clearly has an entire transcript of your conversation."[150]

AIPS also implicate Fourth Amendment concerns. Although the Supreme Court has not directly addressed privacy questions regarding AI surveillance in schools, there is case law that indicates a risk of liability for schools. In the landmark case *New Jersey v. T.L.O.*, the Court found that the Fourth Amendment applies to public school officials as state actors via the Fourteenth Amendment and set forth a framework for school searches.[151] The Court recognized that school settings require "some modification of the level of suspicion of illicit activity needed to justify a search,"[152] and therefore school searches "will be permissible . . . 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."[153] This decision established a two-prong test for schools, shaping how schools approach security.[154] Further, the Court held that a generalized school search without individualized suspicion does not violate students' Fourth Amendment rights if the search is relatively unobtrusive and the nature of the concern is severe because students have a decreased expectation of privacy at school.[155]

However, more recent cases signal a shift toward enhancing privacy protections given advances in technology. In 2008, the Sixth Circuit found the use of video surveillance in schools to be "inherently intrusive" because "a video camera sees all, and forgets nothing."[156] In 2018, the Supreme Court held that location data generated by cell phone towers is protected by the Fourth Amendment,[157] which was a departure from prior adherence to the third-party doctrine.[158] In a case that is perhaps most directly applicable, a district court in Ohio found that a state university's room scans violate students' reasonable expectation of privacy in their homes, making the practice "unreasonable under

150. EPIC Complaint, *supra* note 149.

151. 469 U.S. 325, 333–34 (1985).

152. *Id.* at 340.

153. *Id.* at 342.

154. Weinstein, *supra* note 97, at 462.

155. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 656, 664–65 (1995).

156. Brannum v. Overton Cnty. Sch. Bd., 516 F.3d 489, 496 (6th Cir. 2008). There, thirty-four middle school students sued alleging that school officials violated their Fourth Amendment right to privacy when the officials secretly installed cameras in school locker rooms. *Id.* at 491–92. Using the *T.L.O.* framework, the *Brannum* court found that the school significantly invaded the students' reasonable expectation of privacy since there was nothing in the record about school officials' concerns over student safety or security to reasonably justify the surveillance. *Id.* at 497–99.

157. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

158. Laura Hecht-Felella, *The Fourth Amendment in the Digital Age*, BRENNAN CTR. FOR JUST. (Mar. 18, 2021), https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age.

the Fourth Amendment."[159] Although *Dobbs v. Jackson Women's Health* introduces some uncertainty given that the right to privacy is not explicitly referenced in the Constitution,[160] the district court's opinion strongly signals the potential for the Court to find that AI surveillance in schools violates students' Fourth Amendment privacy rights.

Furthermore, as part of AIPS, students are often recorded in their homes, a place the Fourth Amendment explicitly protects from unreasonable government searches.[161] The move to remote learning has made these search concerns very real, with some dubbing such invasive surveillance "the coronopticon."[162] When recordings are properly reviewed by human proctors, these humans get a peek into the private space of a student. What if the proctor views something they deem as contraband or illegal behavior? What if a child walks by the camera and the parent has not consented to that child being recorded? There have already been at least two instances where teachers thought they observed an African American male student playing with a gun and took disciplinary action that has since been walked back.[163] In one instance, the school sent a sheriff's deputy to the student's home, claiming that the call was out of concern for the student's safety, but the student's family disagreed, suing the school district and claiming that sending officers to their home in fact posed more of a risk to the child.[164] In the other, the student's family sued the district alleging multiple injuries, including a violation of the student's due process rights, resulting from the student's suspension.[165] In yet another case, concerned parents brought a class action lawsuit against Google for violating state privacy rights and COPPA by collecting and storing young students' biometric data through the use of Chromebooks and Google's "G Suite for Education."[166] Those hoping for some

159. Ogletree v. Cleveland State Univ., No. 21-cv-00500, 2022 WL 3581569, at *9 (N.D. Ohio Aug. 22), *amended and superseded by* No. 21-cv-00500, 2022 WL 17826730 (N.D. Ohio Dec. 20, 2022), *appeal filed*, No. 23-3043 (6th Cir. Jan. 18, 2023).

160. *See* 142 S. Ct. 2228, 2242 (2022).

161. U.S. CONST. amend. IV.

162. Jane Bailey, Jacquelyn Burkell, Priscilla Regan & Valerie Steeves, *Children's Privacy Is at Risk with Rapid Shifts to Online Schooling Under Coronavirus*, THE CONVERSATION (Apr. 21, 2020, 10:08 AM), https://theconversation.com/childrens-privacy-is-at-risk-with-rapid-shifts-to-online-schooling-under-coronavirus-135787; *Creating the Coronopticon: Countries Are Using Apps and Data Networks To Keep Tabs on the Pandemic*, THE ECONOMIST (Mar. 26, 2020), https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic.

163. Colette Bordelon, *Following Suspension over Toy Gun in Virtual Class, Family Creates Political Change*, KOAA NEWS (Sept. 15, 2021, 3:54 PM), https://www.koaa.com/news/covering-colorado/following-suspension-over-toy-gun-in-virtual-class-family-creates-political-change; *Louisiana School Board Settles BB Gun Suspension Lawsuits*, AP NEWS (July 9, 2021), https://apnews.com/article/louisiana-education-lawsuits-school-boards-eff45f5b545929742d8dcf5ee830caa5.

164. Rob Low, *12-Year-Old Suspended over Toy Gun Seen in Virtual Class*, KDVR (Sept. 3, 2020, 6:18 PM), https://kdvr.com/news/problem-solvers/12-year-old-suspended-over-toy-gun-seen-in-virtual-class/.

165. Harrison v. Jefferson Par. Sch. Bd., 502 F. Supp. 3d 1088, 1091 (E.D. La. 2020).

166. Class Action Complaint at 3, H.K. v. Google, LLC, No. 20-cv-02257 (N.D. Cal. Apr. 2, 2020).

guidance will be sorely disappointed, as these and similar cases have settled out of court.[167]

Proponents for AIPS argue that students already give up some of their privacy rights when attending school in person, and that AIPS do not differ much from traditional in-person invigilation.[168] In-person proctoring by a complete stranger is a well-established and uncontroversial practice, and is invasive by nature.[169] This has lead some to argue that AI is in some ways better because it can feel less invasive.[170] However, this argument is misled as online proctoring tools generally raise more ethical concerns than in-person proctors.[171] While it is true that students are subjected to some level of oversight, there are differences in the experience and treatment of in-person observation as opposed to online invigilation. An in-person proctor can only concentrate on a few students at a time, whereas with AIPS, all students are scrutinized for the entire exam period. Furthermore, as previously mentioned, AIPS require recording students. This digital data can last indefinitely, with vendors monetizing student "data trails" by creating marketing and advertising profiles of each student.[172] There is also the risk that a reviewer could take a "prurient interest" in the recordings, with the ability to pause, rewind, save, and rewatch the recording for private use.[173] In-person invigilation is safer since human proctors are limited to their own memory and no digital copy of a student's test-taking experience exists.

E. RESPECT FOR AUTONOMY

Another concern critics raise is that AI proctoring will lead impressionable young students to become desensitized to and more accepting of surveillance.[174] The loss of liberty and normalization of invasive tools to conduct surveillance are concerning, especially as AI-based systems become more pervasive.[175]

---

167. *See id.*; *Louisiana School Board Settles BB Gun Suspension Lawsuits*, *supra* note 163; Ryan Warner, *A Year After Sending Cops to a Kid's Home, a Colorado Springs School District Apologizes*, CPR NEWS (Sept. 10, 2021, 6:11 PM), https://www.cpr.org/2021/09/10/a-year-after-sending-cops-to-a-kids-home-a-colorado-springs-school-district-apologizes/; David Kravets, *School District Pays $610,000 To Settle Webcam Spying Lawsuits*, WIRED (Oct. 12, 2010, 4:30 PM), https://www.wired.com/2010/10/webcam-spy-settlement/.

168. Coghlan et al., *supra* note 12, at 1595.

169. *Id.*

170. Chin, *supra* note 56.

171. Coghlan et al., *supra* note 12, at 1599; Nigam et al., *supra* note 17, at 6442.

172. Fedders, *supra* note 84, at 1682–83.

173. Coghlan et al., *supra* note 12, at 1596.

174. *See id.* at 1600; Raso et al., *supra* note 55, at 51; Clive Thompson, *What AI College Exam Proctors Are Really Teaching Our Kids*, WIRED (Oct. 20, 2020, 6:00 AM), https://www.wired.com/story/ai-college-exam-proctors-surveillance/.

175. Nigam et al., *supra* note 17, at 6442; Elizabeth Laird, *Remote Proctoring of Exams Is an Invasive Tool Without Clear Security Protections. States & Districts Should Avoid Rushing In*, THE 74 MILLION (May 18, 2021), https://www.the74million.org/article/laird-remote-proctoring-of-exams-is-an-invasive-tool-without-clear-security-protections-states-districts-should-avoid-rushing-in/.

Schools should provide students opportunities to guard their privacy and give consent, as learning to set boundaries for themselves and others is an essential part of growing up.[176] Instead, critics observe that any "consent" granted to AIPS use does not show a "meaningful exercise of agency" since students are given little actual choice in the school context.[177] Schools should also set the precedent that surveillance is for "particularized occasions" and must be used thoughtfully.[178] According to the International Society for Technology in Education, privacy literacy is essential for students to become digital citizens—they must understand the value of their own data.[179]

Additionally, when an authority figure creates rules without clear definitions, behavior will be chilled if surveillance is also imposed.[180] To avoid punishment, liability, or other negative consequences, individuals will tend to act more conservatively, ultimately resulting in self-censoring.[181] Students have expressed anxiety when taking monitored tests, as they "feel accused by the machine all the time" and are therefore hyper aware of their behavior.[182] Students should feel comfortable in their academic environments rather than constantly preoccupied with being watched. Furthermore, AIPS shape student behavior through punishment, motivating students through fear of negative consequences rather than making an active choice based on their value system.[183] This results in the diminishment of students' abilities to self-regulate or assess risk and reward autonomously.[184]

F. DATA SECURITY

Lastly, one of the biggest worries for AI vendors[185] and organizations considering the adoption of AI is cybersecurity.[186] The amount of data collected

176. Laird, *supra* note 175.

177. Barrett, *supra* note 93, at 698.

178. Fedders, *supra* note 84, at 1722–23.

179. *ISTE Standards: Students*, ISTE, https://www.iste.org/standards/iste-standards-for-students (last visited May 12, 2023).

180. GLOB. NETWORK INITIATIVE, CONTENT REGULATION AND HUMAN RIGHTS POLICY BRIEF 20 (2020), https://globalnetworkinitiative.org/wp-content/uploads/2020/10/GNI-Content-Regulation-HR-Policy-Brief.pdf.

181. *Id.* at 11; *Privacy for Students*, *supra* note 131; Raso et al., *supra* note 55, at 50.

182. EdSurge Podcast, *No Study Groups and Cheating Concerns. Are Students Learning? Pandemic Campus Diaries, Ep. 4*, EDSURGE, at 21:30 (Oct. 6, 2020), https://soundcloud.com/edsurge/no-study-groups-and-cheating-concerns-what-learning-is-like-during-the-pandemic-campus-diaries-ep-4.

183. Fedders, *supra* note 84, at 1710.

184. *Id.* at 1710–11.

185. Michael Chui, Bryce Hall, Alex Singla & Alex Sukharevsky, *The State of AI in 2021*, MCKINSEY & CO. (Dec. 8, 2021), https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2021?cid=emergingtechbrew-pde-pro-mka-oth-2202.

186. STAN. UNIV. HUM.-CENTERED A.I., *supra* note 91, at 163.

is growing exponentially[187] as schools move to gather, create, and maintain student educational records online.[188] Therefore, cybersecurity should be a top priority for educators evaluating digital tools. AIPS, by design, must collect, transmit, and store sensitive data to analyze or make it available for review.[189] This often includes video recordings, IP addresses, ID cards, fingerprints, and face scans.[190] Naturally, there are concerns around how safe the data is in vendors' hands.[191] Cybercriminals have learned that, as a result of the pandemic, student and teacher devices are more connected but less secure,[192] so targeting educational institutions and their proxies has proven remarkably effective.[193] In fact, the pandemic has exacerbated schools' susceptibility to malicious online activity,[194] and according to Microsoft Security Intelligence data, education as an industry has suffered the most enterprise-level malware attacks.[195] The Government Accountability Office says the United States' "education facilities are inherently at risk,"[196] and cybersecurity researchers call public K-12 schools "sitting ducks," warning that "[t]he threat is increasing, not decreasing"[197] due to minimal funding, lack of training, and exhausted staff.[198]

187. Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 354 (2015).

188. Fedders, *supra* note 84, at 1713.

189. Raso et al., *supra* note 55, at 50; Nigam et al., *supra* note 17, at 6423.

190. Nigam et al., *supra* note 17, at 6439.

191. Raso et al., *supra* note 55, at 54.

192. Alyson Klein, C*yberattacks on Schools Soared During the Pandemic*, EDUC. WK. (Mar. 10, 2021), https://www.edweek.org/technology/cyberattacks-on-schools-soared-during-the-pandemic/2021/03.

193. Alyson Klein, *Thousands of School Websites Went Down in a Cyberattack. It'll Happen Again, Experts Say*, EDUC. WK. (Jan. 10, 2022), https://www.edweek.org/technology/thousands-of-school-websites-went-down-in-a-cyberattack-itll-happen-again-experts-say/2022/01; *Cyber Actors Target K-12 Distance Learning Education To Cause Disruptions and Steal Data*, CISA, https://www.cisa.gov/uscert/ncas/alerts/aa20-345a (Dec. 10, 2020).

194. Nir Kshetri, *Cybercriminals Use Pandemic To Attack Schools and Colleges*, GOV'T COMPUT. NEWS (Sept. 15, 2021), https://gcn.com/cybersecurity/2021/09/cybercriminals-use-pandemic-to-attack-schools-and-colleges/316131/; Jenni Bergal, *Cybercriminals Strike Schools amid Pandemic*, PEW CHARITABLE TRS.: STATELINE (Sept. 22, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/09/22/cybercriminals-strike-schools-amid-pandemic; *see also The K-12 Cyber Incident Map*, K12 SIX, https://www.k12six.org/map (Feb. 13, 2023).

195. *Global Threat Activity*, MICROSOFT: MICROSOFT SEC. INTEL., https://www.microsoft.com/en-us/wdsi/threats (last visited May 12, 2023) (showing that "Education" as an industry made up over 80% of the reported malware encounters in the last thirty days).

196. Mitch Blacher, *Hackers Target Students, Costing Schools Hundreds of Millions in System Downtime*, ABC NEWS (Dec. 13, 2021, 12:35 PM), https://wjla.com/features/investigations/hackers-target-student-records-costing-schools-hundreds-millions-system-downtime-names-social-security-numbers-grades-addresses-washington-dc-threats.

197. Lindsay McKenzie, *Colleges a 'Juicy Target' for Cyberextortion*, INSIDE HIGHER ED (Mar. 19, 2021), https://www.insidehighered.com/news/2021/03/19/targeting-colleges-and-other-educational-institutions-proving-be-good-business.

198. Dan Patterson, *Schools Have Become the Leading Targets of Ransomware Attacks*, CBS NEWS (Mar. 11, 2021, 12:00 PM), https://www.cbsnews.com/news/schools-popular-ransomware-targets/.

Security experts have also expressed concerns around mandating students to download AIPS software onto their personal devices, particularly ones that give full remote access to a stranger.[199] One of these experts, vice president of ExpressVPN Harold Li, explains that "[a]t a minimum, it sets a bad precedent and establishes dangerous security habits."[200] Other critics liken AIPS to a computer virus[201] or malware,[202] given the depth and breadth of access the software has to a test-taker's device.

These fears have come to fruition with at least one AIPS vendor, ProctorU, reporting a data breach in July 2020.[203] Security consultants also detected a vulnerability in a different AIPS vendor's browser extension.[204] The vulnerability put anyone who had the software installed at risk of having all of their browser activity surreptitiously observed.[205] Although the vendor patched the vulnerability within a week of being notified, it was exploitable for months beforehand.[206] Some AIPS vendors have attempted to address this concern in their marketing, featuring blogposts that expound upon all the ways their product meets a school's security needs.[207] But just because the marketing materials claim certain protections does not guarantee that those protections are reflected in actual vendor policy and behavior. These additional risks are unavoidable and inherent to implementation of any online tool.

III. POLICY & PROTECTIONS

A. CURRENT POLICIES

While there are constitutional and statutory provisions that prohibit discrimination against students on the basis of race or disability, the protections they provide are inadequate to address all of the potential harms AI proctoring

199. Chin, *supra* note 56.

200. *Id.*

201. Jake Binstein, *To E-Proctor or Not To E-Proctor Webinar*, JAKE BINSTEIN BLOG, at 12:30 (Nov. 19, 2020), https://jakebinstein.com/blog/to-e-proctor-or-not-to-e-proctor-webinar/.

202. Swaak, *supra* note 36.

203. Sarah Coble, *Online Exam Tool Suffers Data Breach*, INFOSEC. MAG. (Aug. 6, 2020), https://www.infosecurity-magazine.com/news/online-exam-tool-suffers-data/; @ProctorUSupport, TWITTER (Aug. 6, 2020, 12:04 PM), https://twitter.com/ProctorUSupport/status/1291450175815286786.

204. Coble, *supra* note 203.

205. *Students Vulnerable for Months Due to Leak in Proctorio*, CYBERTHREAT INTEL. (Dec. 16, 2021), https://cyberthreatintelligence.com/news/students-vulnerable-for-months-due-to-leak-in-proctorio/ [https://web.archive.org/web/20211221101640/https://cyberthreatintelligence.com/news/students-vulnerable-for-months-due-to-leak-in-proctorio/].

206. *Id.*

207. *Online Proctoring and Protecting Student Privacy: The Best of Both Worlds*, PROCTORTRACK (June 17, 2020, 1:56 PM), https://www.proctortrack.com/blog/article/online-proctoring-and-protecting-student-privacy-the-best-of-both-worlds/.

can pose.[208] Critics of AIPS point out that current laws regarding children's information offer little protection, primarily because they were passed before AI became widespread.[209] The proliferation of online surveillance technologies suggests that existing statutes and judicial precedent do not provide sufficient regulation to keep pace with developing technologies.[210] Although states have passed their own legislation addressing general student-privacy concerns,[211] only a few states have laws regulating commercial use of biometrics.[212] Additionally, although the number of proposed federal AI-related bills shot up from one in 2015 to 130 in 2021,[213] the current federal landscape of legal protections focused on student privacy and data remains minimal and surprisingly inapplicable to much of the student data schools and private vendors collect.[214] For example, the Family Educational Rights and Privacy Act ("FERPA") controls the manner of receipt and categories of recipients of student educational records.[215] COPPA requires parental consent for data collection of children thirteen and under.[216] The Protection of Pupil Rights Amendment of 1978 ("PPRA") is the final federal student data and privacy regulation, but as it applies only to situations where a school is providing student survey information to a third party for marketing purposes, it is irrelevant to AIPS and will not be discussed here.[217] While these laws all serve important policies, none of them adequately address the concerns raised in Part II, indicating a gap in the government's effective regulation of an increasingly digital educational ecosystem.

---

208. Barrett, *supra* note 93, at 740.

209. LU & HARRIS, *supra* note 16, at 2.

210. Fedders, *supra* note 84, at 1718.

211. *See State Student Privacy Laws*, STUDENT PRIV. COMPASS, https://studentprivacycompass.org/state-laws/ (last visited May 12, 2023).

212. Natalie A. Prescott, *The Anatomy of Biometric Laws: What U.S. Companies Need To Know in 2020*, THE NAT'L L. REV. (Jan. 15, 2020), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020; *see* Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14/10 to 14/15 (West 2022); WASH. REV. CODE ANN. § 19.375.020 (West 2022); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2022).

213. STAN. UNIV. HUM.-CENTERED A.I., *supra* note 91, at 178; *see, e.g.*, Khari Johnson, *Congress Introduces Bill That Bans Facial Recognition Use by Federal Government*, VENTUREBEAT (June 25, 2020, 12:32 PM), https://venturebeat.com/2020/06/25/congress-introduces-bill-that-bans-facial-recognition-use-by-federal-government/ (describing the Facial Recognition and Biometric Technology Moratorium Act of 2020, S. 4084, 116th Cong. (2020)).

214. Strauss, *supra* note 88.

215. Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

216. LU & HARRIS, *supra* note 16, at 2.

217. Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h; *What Is the Protection of Pupil Rights Amendment (PPRA)?*, U.S. DEP'T OF EDUC., https://studentprivacy.ed.gov/faq/what-protection-pupil-rights-amendment-ppra (last visited May 12, 2023). The PPRA is not relevant to AIPS concerns because the statute only applies to the "collection, disclosure, or use of personal information collected from students for the purpose of marketing or [sale]" and the ability for a student to opt out of surveys or physical screenings. § 1232h(c)(1)(E).

1. Family Educational Rights and Privacy Act

FERPA was passed in 1974 to protect the confidentiality of student educational records and provide parents transparency and access to their students' information.[218] FERPA has been amended eleven times as Congress and the Department of Education have recognized new situations in which personally identifiable information can be disclosed without explicit parent or student consent,[219] but is still criticized for its "pre-Internet approach to data that is out of touch with today's modern and digitally connected classroom."[220] In 2008, the Department of Education expanded its regulatory definition of "personally identifiable information" ("PII") to include students' "biometric records," which includes fingerprints, iris patterns, facial characteristics, voiceprints, and handwriting.[221] While this would, in theory, provide the needed protection, Congress simultaneously also removed the strict limitations on nonconsensual disclosure of PII in a "health or safety" emergency.[222] The 2013 amendments further diluted students' protections by creating a "school official" exception, permitting schools to share data with third parties for operational needs like testing without any notification to parents or students.[223] Additionally, because FERPA only applies to schools and not the third-party vendors schools partner with, it does not regulate how the companies use student data, nor can it hold them accountable.[224] And even though the Department of Education can sanction educational institutions, it has never chosen to do so.[225]

Even if FERPA had provided the protections students hoped for, the Supreme Court in *Gonzaga University v. Doe* held that individual students and organizations cannot sue to enforce FERPA because the statute does not have a clear and unambiguous creation of an individual right.[226] Given the limited threat

---

218. *See* Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 57 (codified as amended at 20 U.S.C. § 1232g); *Family Educational Rights and Privacy Act (FERPA)*, ELEC. PRIV. INFO. CTR., https://epic.org/family-educational-rights-and-privacy-act-ferpa/ (last visited May 12, 2023).

219. *Family Educational Rights and Privacy Act (FERPA)*, *supra* note 218.

220. FED. COMM'N ON SCH. SAFETY, U.S. DEP'T OF EDUC., FED. COMM'N ON SCH. SAFETY: PROTECT & MITIGATE 129 (2018), https://www2.ed.gov/documents/school-safety/school-safety-report.pdf; *see also* Fedders, *supra* note 84, at 1682.

221. Personally Identifiable Information and De-Identified Records and Information, 73 Fed. Reg. 74829, 74833 (Dec. 9, 2008) (to be codified at 94 C.F.R. § 99.3).

222. FED. COMM'N ON SCH. SAFETY, *supra* note 220, at 131.

223. Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (Oct. 5, 2013), https://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html; *see also* Kevin Miller, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. TECH. L. & POL'Y 105, 112 (2014); Barrett, *supra* note 93, at 738; Fedders, *supra* note 84, at 1683–84.

224. Barrett, *supra* note 93, at 738 (explaining that FERPA only provides the ability to sanction the educational institution and not the vendor itself).

225. Elana Zeide, *The Limits of Education Purpose Limitations*, 71 U. MIAMI L. REV. 494, 503 (2017); Jordan Clark, *Does FERPA Impact Edtech Companies?*, EDLINK (Mar. 3, 2020), https://ed.link/community/ferpa/.

226. 536 U.S. 273, 290 (2002).

of enforcement, schools have little incentive to comply.[227] Moreover, in *S.A. ex rel L.A. v. Tulare County Office of Education*, the district court held that emails stored on teachers' private hard drives did not constitute educational records until they were centrally located.[228] This implies that data that is collected online but not maintained by the school (what AIPS collect) is not covered under FERPA. Indeed, critics of FERPA point out its unclear language regarding what counts as an educational record, particularly when it comes to data that new technologies generate.[229]

2. Children's Online Privacy Protection Act & the Federal Trade Commission

COPPA generally requires that companies provide notice and obtain parental consent to collect personal information from children.[230] However, the statute does not address broader student concerns about AIPS because it only applies to service providers that collect the personal data of students younger than age thirteen.[231] Additionally, like FERPA, COPPA permits schools to consent on behalf of parents to the collection of student data by the services the schools utilize.[232] And like FERPA, COPPA does not grant a private right of action—only the FTC and state and federal governments can enforce the law.[233] Unlike FERPA, however, the FTC has taken legal action in the past year to enforce COPPA, bringing lawsuits against app developers like HyperBeard, Inc. for collecting personal data without parental consent from children under thirteen, and Miniclip, S.A. for misleading customers into thinking it was part of a COPPA safe harbor program when it was not.[234] Though these suits show that the FTC is enforcing student privacy statutes and has ramped up efforts to "stop bad actors from exploiting the pandemic at the public's expense,"[235] they also show that the FTC is focused more broadly on punishing misleading and misrepresentative communications than on enforcing COPPA, thereby incentivizing companies to simply be more careful with their advertising rather than actually creating responsible data and privacy policies.

---

227. Susan G. Archambault, *Student Privacy in the Digital Age*, 2021 BYU EDUC. & L.J. 1, 30.

228. No. CV F 08-1215, 2009 WL 30298, at *5 (E.D. Cal. Jan. 6, 2009).

229. *See, e.g.*, Fedders, *supra* note 84, at 1683.

230. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

231. *See id.* § 6501.

232. Lisa Weintraub Schifferle, *Remote Learning and Children's Privacy*, FED. TRADE COMM'N (Apr. 9, 2020), https://consumer.ftc.gov/consumer-alerts/2020/04/remote-learning-childrens-privacy.

233. *Complying with COPPA: FAQ*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#B.%20COPPA%20Enforcement (last visited May 12, 2023).

234. FTC, PROTECTING CONSUMERS DURING THE COVID-19 PANDEMIC: A YEAR IN REVIEW 10 (2021), https://www.ftc.gov/reports/protecting-consumers-during-covid-19-pandemic-year-review.

235. *Id.* at 14.

This functionality of upholding consumer protection laws could provide the enforcement mechanisms necessary to dissuade AIPS vendors from using test-taker data in misleading ways. The FTC, as part of its ability to regulate "unfair or deceptive acts or practices" under section 18 of the Federal Trade Commission Act, has the authority to hold accountable companies that lie or fail to fully disclose their data, security, and privacy practices.[236] The FTC also appears to be the only agency attempting to limit discriminatory AI and privacy violations.[237] It is considering new regulations to ban certain kinds of AI practices and to provide more guidelines to companies on how to properly use AI and automated decision systems.[238] It has also acknowledged that student privacy breaches are "materially consequential."[239] In April 2021, the FTC advised companies to look out for discriminatory outcomes, embrace independence, be honest and accurate about what their products do, be transparent about their data use, "[d]o more good than harm," and hold themselves accountable or "be ready for the FTC to do it for [them]."[240] However, the FTC is only one agency with finite resources, so companies will likely only be examined if someone sues.[241]

3. Office for Civil Rights

Finally, from the Author's experience,[242] although the Department of Education's Office for Civil Rights enforces several laws that protect students from discriminatory treatment from educational institutions that receive federal funding,[243] it does not yet have a remedy for students who bring discrimination complaints about AIPS' inability to recognize their faces. Moreover, it is unlikely that a student would be able to bring a successful Fourteenth

236. FTC, FTC POLICY STATEMENT ON UNFAIRNESS (1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

237. *Cost of Proposed US AI Bill May Outweigh Its Benefits*, PYMNTS (Feb. 10, 2022), https://www.pymnts.com/news/regulation/2022/cost-of-proposed-us-ai-bill-may-outweigh-its-benefits/.

238. *Id.*

239. Lina M. Khan, Chair, Fed. Trade Comm'n, Remarks as Prepared for Delivery at the IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf.

240. Elisa Jillson, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI*, FED. TRADE COMM'N (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai.

241. *Cf.* EPIC Complaint, *supra* note 149. In December 2020, the Electronic Privacy Information Center filed a complaint against five major AIPS vendors alleging unfair and deceptive trade practices for collecting excessive personal data from students. *See generally id.*

242. The Author externed at the Department of Education, Office for Civil Rights during the summer of 2021.

243. This includes Title VII for race, gender, ethnicity, color, and national origin, and section 504 and Title II for disability. *About OCR*, U.S. DEP'T OF EDUC. OFF. FOR C.R., https://www2.ed.gov/about/offices/list/ocr/aboutocr.html (Nov. 7, 2022).

Amendment equal protection claim based on alleged discriminatory treatment from AIPS because the Supreme Court has held that for disciplinary challenges of an online activity, statistical evidence without discriminatory purpose or intent is not enough.[244]

B. FUTURE POLICIES

In July 2022, the House Energy & Commerce Committee advanced the "American Data Privacy and Protection Act" ("ADPPA"), a comprehensive data security and digital privacy measure, with bipartisan support.[245] ADPPA seeks to increase transparency, providing guidelines on how individuals access, correct, and delete the data that covered entities have on them, as well as limiting the use of minors' data, protecting sensitive data, promoting data minimization efforts,[246] and improving oversight of AI algorithmic decisionmaking.[247]

Moreover, in February 2022, legislation was introduced in both the House and Senate—H.R. 6580[248] and S. 3572,[249] respectively—proposing FTC oversight of automatic AI processes.[250] The bills, titled the "Algorithmic Accountability Act of 2022" (the "Act"), specify that vendors must "eliminate or mitigate, in a timely manner, any impact made by an augmented critical decision process that demonstrates a likely material negative impact that has legal or similarly significant effects on a consumer's life."[251] While the Act shows movement in a much needed direction, it would only apply to those companies with revenues greater than $50 million or more than $250 million in market capitalization, so even the very largest vendors in the space may not be affected.[252] It also seems unlikely that an AI proctor flagging a student's behavior would rise to the level of being considered a "material negative impact" in most low-stakes testing situations, and therefore the Act, if passed, would not have much effect on protecting students' rights on this particular issue.

244. Amy B. Cyphert, *Addressing Racial Disparities in Preschool Suspension and Expulsion Rates*, 82 TENN. L. REV. 893, 916 (2015).

245. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

246. *Id.*

247. Niketa K. Patel, Tori K. Shinohara, Jennifer M. Rosa, Brendan J. Harrington, Arsen Kourinian & Howard W. Waltzman, *The American Data Privacy and Protection Act: Is Federal Regulation of AI Finally on the Horizon?*, MAYER BROWN (Oct. 21, 2022), https://www.mayerbrown.com/en/perspectives-events/publications/2022/10/the-american-data-privacy-and-protection-act-is-federal-regulation-of-ai-finally-on-the-horizon.

248. Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022).

249. Algorithmic Accountability Act of 2022, S. 3572, 117th Cong. (2022).

250. Kristin L. Bryan, Kyle R. Fath & Gicel Tomimbang, *Federal Lawmakers in House and Senate Introduce Algorithmic Accountability Act of 2022*, THE NAT'L L. REV. (Feb. 11, 2022), https://www.natlawreview.com/article/federal-lawmakers-house-and-senate-introduce-algorithmic-accountability-act-2022.

251. H.R. 6580 § 3(H); S. 3572 § 3(H).

252. *See generally* MKT. RSCH., GLOBAL REMOTE PROCTORING SOLUTIONS MARKET SIZE, STATUS AND FORECAST 2020–2026 (2020).

However, if AIPS are used to authenticate a student's identity or to determine if a student is cheating on a high-stakes test, the vendor would likely have to comply with the proposed regulation since those decisions and judgements arguably do have a legal, material, or other significant effect on a student's life.[253]

The Act would also require companies to assess the privacy and security risks of their automated systems, and to train, educate, and support their employees on these matters,[254] which indicates that the legislature understands the growing dangers technology brings. It also enjoys support from a multitude of technology experts and civil society organizations, so there appears to be consensus around the desire for federal regulation of AI.[255] If applicable to AIPS vendors, this Act would provide a level of protection for students that currently does not exist. However, even if the Act were to pass, it would still be at least three to four years before the FTC would promulgate regulations and start enforcement.[256] Further, critics worry that although the Act is a good first step in regulating AI bias and security, the cost to companies may be significant and will not prevent the most harmful practices since the FTC will still have to investigate all potential violations.[257]

There appears to be momentum for privacy legislation as President Biden has signaled a ramp up of protections for children, explicitly referring to children's privacy in his 2022 State of the Union address.[258] A White House press release on Biden's administrative agenda stated that he planned to call for banning excessive data collection and the use of discriminatory algorithmic decisionmaking.[259] Additionally, the SEC has indicated that it will consider a cybersecurity proposal to amend regulations that will likely affect public

253. Bryan et al., *supra* note 250.

254. Justin Hendrix, *Lawmakers Introduce Algorithmic Accountability Act*, TECH POL'Y PRESS (Feb. 3, 2022), https://techpolicy.press/senators-introduce-algorithmic-accountability-act/.

255. *See* Press Release, Sen. Ron Wyden, Wyden, Booker and Clarke Introduce Algorithmic Accountability Act of 2022 To Require New Transparency and Accountability for Automated Decision Systems (Feb. 03, 2022), https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems.

256. Bryan et al., *supra* note 250.

257. *Cost of Proposed US AI Bill May Outweigh Its Benefits*, *supra* note 237.

258. Kristin Bryan, Kyle Fath & Elizabeth Berthiaume, *Privacy Continues To Be Top of Mind Issue with President Biden's State of the Union Address and Movement on FTC Nominee Today*, PRIV. WORLD (Mar. 3, 2022), https://www.privacyworld.blog/2022/03/privacy-continues-to-be-top-of-mind-issue-with-president-bidens-state-of-the-union-address-and-movement-on-ftc-nominee-today/.

259. *Id.*

companies.[260] However, proposed legislation does not always come to fruition, and multiple attempts at regulating the AI industry have already failed.[261]

C. RECOMMENDED PRACTICES

Consulting firms recommend standardization of practices and model documentation as emerging best practices for AI risk mitigation.[262] In response to Executive Order 13859 in February 2019,[263] the National Institute of Standards and Technology ("NIST") started to create technical standards that "reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies and develop international standards to promote and protect those priorities."[264] NIST explains that the standards-development process in the United States relies heavily on the private sector to develop "voluntary consensus standards" to remain consistent with the United States' "market-driven economy[,] and has been endorsed in Federal statute and policy."[265] Additionally, organizations like the Organisation for Economic Co-Operation and Development ("OECD") recommend that government and private sectors cooperate with each other to develop "multi-stakeholder, consensus-driven global technical standards for interoperable and trustworthy AI."[266] Further, the International Organization for Standardization ("ISO") has put out recommendations for improving the trustworthiness of AI technologies.[267] However, industry leaders refusing to opt in to voluntary initiatives like the Safe Face Pledge is evidence that direct regulation of private industry is needed.[268]

260. *Open Meeting Agenda - March 9, 2022: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/os/agenda-open-030922 (Mar. 11, 2022).

261. *See, e.g.*, Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019); Student Privacy Protection Act, H.R. 3157, 114th Cong. (2015); *see also* Anokhy Desai, *US State Privacy Legislation Tracker*, IAPP, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last visited May 12, 2023).

262. Buehler et al., *supra* note 88.

263. Exec. Order No. 13,859, 84 Fed. Reg. 3967 (Feb. 14, 2019).

264. NAT'L INST. OF STANDARDS & TECH., U.S. LEADERSHIP IN AI: A PLAN FOR FEDERAL ENGAGEMENT IN DEVELOPING TECHNICAL STANDARDS AND RELATED TOOLS 7 (2019), https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

265. *Id.* at 9.

266. ORGANISATION FOR ECON. CO-OPERATION & DEV., *supra* note 88, at 9.

267. Elizabeth Gasiorowski-Denis, *Towards a Trustworthy AI*, ISO (July 7, 2020), https://www.iso.org/news/ref2530.html.

268. Joy Buolamwini & Sasha Costanza-Chock, *Announcing the Sunset of the Safe Face Pledge*, MEDIUM (Feb. 8, 2021), https://medium.com/@Joy.Buolamwini/announcing-the-sunset-of-the-safe-face-pledge-36e6ea9e0dc5.

IV. PROPOSED SOLUTIONS

A. ALTERNATIVE SOLUTIONS TO AIPS USAGE & REMOTE PROCTORING GENERALLY

In an ideal world, the best solution for all the above concerns is simply to stop using AIPS. Technology is often thought of as a panacea to the many struggles of educators. However, without careful planning and consideration, a poorly implemented tool can cause more harm than it solves. An abundance of alternative methods to evaluating knowledge and learning exist, making conventional high-stakes, end-of-course assessments unnecessary altogether.[269] Cognitive psychologists have generally rejected the efficacy of rote memorization when it comes to deep learning and recommend that educational institutions emphasize students' abilities to analyze, evaluate, and create in order to gain true comprehension and mastery over a subject.[270] These nontraditional assignments also have the benefit of increasing student motivation and engagement.[271] Many educators are championing techniques like an increased number of opportunities for practice in the form of short daily quizzes or series of tests;[272] longer, more comprehensive assignments that require synthesis of student work[273] such as research projects, papers, and poster sessions;[274] assessments with peer feedback;[275] and simply giving open-book,[276] open-world exams where proctoring would be extraneous.[277] Opportunities for students to use concept-mapping to test higher-order thinking have also been successful, receiving positive student feedback.[278]

---

269. *Alternatives to Traditional Exams and Papers*, IND. UNIV. BLOOMINGTON, https://citl.indiana.edu/teaching-resources/assessing-student-learning/alternatives-traditional-exams-papers/index.html (last visited May 12, 2023) (describing test alternatives for different kinds of knowledge assessment).

270. Chaelin Jung, *Big Ed-Tech Is Watching You: Privacy, Prejudice, and Pedagogy in Online Proctoring*, BROWN POL. REV. (Dec. 6, 2020), https://brownpoliticalreview.org/2020/12/big-ed-tech-is-watching-you-privacy-prejudice-and-pedagogy-in-online-proctoring/.

271. *Alternatives to Traditional Exams and Papers*, *supra* note 269.

272. *Tips for Exams and Alternative Assessments*, RUTGERS SCH. OF ARTS & SCIS., https://sasoue.rutgers.edu/teaching-learning-guides/remote-exams-assessment#special-advice-for-open-book-assessment-in-quantitative-courses (last visited May 12, 2023).

273. Wrynn Memorandum, *supra* note 81, at 2.

274. *Alternatives to Traditional Testing*, BERKELEY CTR. FOR TEACHING & LEARNING, https://teaching.berkeley.edu/resources/course-design-guide/design-effective-assessments/alternatives-traditional-testing (last visited May 12, 2023).

275. Alyson Klein, *How To Prevent Student Cheating During Remote Learning: 4 Tips*, EDUC. WK. (Aug. 25, 2020), https://www.edweek.org/teaching-learning/how-to-prevent-student-cheating-during-remote-learning-4-tips/2020/08.

276. Swaak, *supra* note 36.

277. Lederman, *supra* note 41.

278. Karinda Barrett, *A Different Kind of Final*, FAC. FOCUS (Oct. 15, 2013), https://www.facultyfocus.com/articles/educational-assessment/a-different-kind-of-final/ (describing student feedback that the method helped make the lessons stick, and was "[m]uch better than regular exams, more fun . . . [and] less pressure").

Additionally, as COVID-19 outbreaks wane, school districts are reexamining their finances and are finding that an online education is not only "academically hazardous" for students, but also financially unsustainable.[279] As schools transition back to in-person learning, schools should find people-centered rather than technology-centered solutions.[280] For the amount of money spent on AIPS, schools could hire a team of educational technologists and instructional design staff, or focus those funds on faculty professional development to help educators create more authentic assessments independently.[281]

Some AIPS vendors argue that these alternatives do not lend themselves to the kind of work STEM classes require, citing the difficulty of making a mathematics final paper or project relevant.[282] However, groups of educators have found creative ways to assess student learning for all content areas using ePortfolios[283] and other similar presentation methods.[284] Other methods to assess learning for quantitative courses include asking students to identify errors in proofs or computations and to apply their knowledge by setting up problems correctly.[285]

If schools really believe giving online exams is the best option, there are also ways to curb cheating that do not require AIPS, and engineers are attempting to create new systems that are less intrusive.[286] One solution is to simply return to a more traditional method of proctoring by using nonrecorded Zoom rooms.[287] Other online testing strategies suggested by experts avoid proctoring altogether. By keeping exams open for a twenty-four-hour period, students have the flexibility to take the exam at the time that works for them on a particular day, and the twenty-four-hour limitation restricts cheating because it lessens the amount of time students have to discuss exam questions with those

279. Mark Lieberman, *One Big Reason Schools Are Ditching Remote Learning: The Cost*, EDUC. WK. (June 7, 2021), https://www.edweek.org/leadership/one-big-reason-schools-are-ditching-remote-learning-the-cost/2021/06.

280. Sarah Silverman, Autumm Caines, Christopher Casey, Belen Garcia de Hurtado, Jessica Riviere, Alfonso Sintjago & Carla Vecchiola, *What Happens when You Close the Door on Remote Proctoring? Moving Toward Authentic Assessments with a People-Centered Approach*, 39 TO IMPROVE ACAD. 115, 118 (2021).

281. S*ee id.* at 125.

282. *Top 9 Remote Proctoring Benefits for Universities—and Their Students*, *supra* note 41.

283. Helen L. Chen, *AAEEBL Meetup April 2020: Evidence of Student Learning*, ASS'N OF AUTHENTIC, EXPERIENTIAL & EVIDENCE-BASED LEARNING (Apr. 4, 2020), https://aaeebl.org/2020/04/04/aaeebl-april-2020-meetup/.

284. *Alternatives to Traditional Testing*, *supra* note 274 (describing student presentations similar to the kind a "professional consultant" would give, and poster sessions with peer critique).

285. *Tips for Exams and Alternative Assessments*, *supra* note 272.

286. Tharun Komari, *How AI Can Spot Cheating Without Breaching Student Privacy*, REWIRE MAG., https://rewire.ie.edu/ai-spot-cheating-breaching-student-privacy (last visited May 12, 2023) (describing an AIPS that does not use face or voice detection).

287. Claburn, *supra* note 120.

who have not taken it yet.[288] Showing only one question at a time and preventing students from re-accessing them also limits cheating.[289] Requiring students to sign an academic integrity contract[290] and creatively reminding students of the policy can also serve schools well, as does delaying test score reporting and protecting test question answers by only revealing the questions and answers the student answered incorrectly.[291] Avoiding online proctoring altogether allows for the safest, most fair testing solution.

B. PROPOSED REGULATION: A NEW KIND OF PRIVACY RIGHT

If halting online testing is not feasible, government oversight is the next best solution. Tiffany Li, in her article *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, proposes the idea of educational privacy,[292] positing that the shift to online learning has muddied the boundaries between school and home, causing students to miss out on the safe space to freely explore private ideas that physically going to school provided.[293] Without this separation, students are no longer shielded from the interference of family, which can lead to a significant loss of psychological and physical safety.[294] Additionally, many students are children, and children are readily recognized as deserving a higher standard of care by U.S. and international jurisprudence.[295] Education is also recognized as an important human right by the international

288. San Jose State Univ. Ctr. for Fac. Dev., *Tips to Transition to Online Exams*, *Mary Poffenroth (Faculty, Biological Sciences)*, YOUTUBE (Mar. 26, 2020), https://www.youtube.com/watch?v=OuBD51-AjB8&app=desktop.

289. *Id.*

290. *See* Berkeley Memorandum, *supra* note 82, at 2.

291. Stephanie Smith Budhai, *Fourteen Simple Strategies To Reduce Cheating on Online Examinations*, FAC. FOCUS (May 11, 2020), https://www.facultyfocus.com/articles/educational-assessment/fourteen-simple-strategies-to-reduce-cheating-on-online-examinations/.

292. Tiffany C. Li, *Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis*, 52 LOY. U. CHI. L.J. 767, 791 (2021).

293. *Id.* at 794.

294. *Id.*

295. *See, e.g.*, Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506; Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, art. 7, 8, 2016 O.J. (L 119) [hereinafter General Data Protection Regulation]; *Children's Code: Best Interests Framework*, ICO., https://ico.org.uk/for-organisations/children-s-code-best-interests-framework/ (last visited May 12, 2023); G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 25(2) (Dec. 10, 1948) (explaining that "childhood [is] entitled to special care and assistance"); G.A. Res. 44/25, Convention on the Rights of the Child, art. 29 (Nov. 20, 1989) (describing how the development of children's personalities, talents, and mental and physical abilities should be nurtured to their fullest potential so that they will be prepared to live life in a "free society"); G.A. Res. 44/25, *supra*, at art. 16(1) (calling for no "arbitrary or unlawful interference with his or her privacy").

community;[296] by extension, students should enjoy a higher standard of privacy in that setting. In this way, an educational privacy right is essentially a welfare or developmental right[297]—a right that the United States may not be legally bound to create but should as a moral imperative. Students also have very little say regarding the privacy practices of their school systems, so this lack of control further implicates a need for an alternative privacy right.[298]

The issues AI proctoring raises are many, and thus far the government, schools, and AIPS vendors have not taken sufficient steps to protect students. To ameliorate this situation, and in lieu of completely discontinuing AIPS usage, a two-pronged approach to providing a safe environment for children that balances the need for academic integrity and administrability with respect for students' privacy should be implemented. First, as described below, regulations at the federal level must be put in place to motivate private actors to create proper safeguards in their AI proctoring products—a comprehensive vendor-centered, top-down approach. Second, educational institutions should be accountable and responsible for considering a host of AI ethics principles when deciding whether to adopt AIPS—a school-centered, bottom-up approach. Ideally, the different constituencies within a school's ecosystem will come together to form a working group where multiple perspectives are considered. Additionally, these prongs would be buttressed by the creation of a special privacy right for education allowing both vendors and institutions to delineate the standards of proper conduct within the education sphere.

1. Prong 1: Regulations & a Vendor-Centered Approach

In countries where remote learning has been successful, public-private partnerships have been highly effective in building such learning environments.[299] Given the potential for growth and advancement of educational tools via AI, this new educational privacy right would incentivize vendors to comply with a higher standard of protections and assurances that are grounded in international AI ethics standards. It would also allow laws to be narrowly tailored specifically for the educational space, giving regulators the flexibility to be more stringent in their demands of private vendors and schools.[300] Activist groups in the space also recommend that a federal authority have oversight as

296. G.A. Res. 44/25, *supra* note 295, at art. 28 (describing the right of the child to a primary, compulsory, and free education).

297. Fedders, *supra* note 84, at 1708.

298. Li, *supra* note 292, at 800.

299. SUSY NDARUHUTSE, EMMA GIBBS & RACHEL FITZPATRICK, EDUC. DEV. TR., WHAT ARE COUNTRIES DOING THAT ALREADY USE REMOTE LEARNING EXTENSIVELY? WHAT CAN WE LEARN FROM THEM? 29 (2020), https://edtechhub.org/wp-content/uploads/2020/09/What-are-countries-that-already-use-remote-learning-doing-and-what-can-we-learn-from-them-EdTechHub.pdf.

300. Li, *supra* note 292, at 804.

well as dedicated expertise in the technologies and risks they pose in various applications.[301]

Taking a cue from the European Union's General Data Protection Regulation ("GDPR"),[302] a policy should be created that requires AIPS vendors to meet several obligations before their product can even reach the market. These obligations include operational requirements like the implementation of a risk-management system, clear data governance, technical documentation, thorough recordkeeping, security, feedback loops, and the resources and processes to correct identified issues as they arise, ensuring accurate outputs. Further, EdTech vendors should adhere to the philosophical ideals of transparency and accountability. This means that all educational data collection and analysis should be visible, traceable, and auditable by stakeholders.[303] A student should have the right to know the logic behind why an automated decision came out the way it did, and vendors should reveal how the inputs were used if a student challenges the decision.

Additionally, as recommended by a United Nations report, vendors should also strive to incorporate the principles of data minimization and privacy by design and default.[304] As a best practice, AIPS vendors should carefully evaluate how each category of risk could manifest from each AI tool they provide.[305] Monitoring the system's results is also necessary to ensure that outputs are not biased.[306] In addition to these practical items, a policy similar to article 22 of the GDPR[307] that prohibits students from being subject to a decision that significantly affects them based solely on an automated process should be implemented. This is often referred to as keeping the "humans in the loop" to ensure that the context of a situation is taken into account.[308]

To create meaningful, effective regulations, an interdisciplinary working group consisting of experts from the EdTech industry, academia, students, educators, engineers, and data scientists should be formed to ensure all impacted stakeholder perspectives are considered. Conversations related to AI ethics, the tension between school needs and student rights, and the impact these

301. ERIK LEARNED-MILLER, VICENTE ORDÓÑEZ, JAMIE MORGENSTERN & JOY BUOLAMWINI, ALGORITHMIC JUST. LEAGUE, FACIAL RECOGNITION TECHNOLOGIES IN THE WILD: A CALL FOR A FEDERAL OFFICE 38 (2020), https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf.

302. General Data Protection Regulation, *supra* note 295, at arts. 7–8; *see also* Colonna, *supra* note 88, at 30–32.

303. MIAO ET AL., *supra* note 6, at 33.

304. OFF. OF THE UNITED NATIONS HIGH COMM'R FOR HUM. RTS., *supra* note 85, at 14.

305. Buehler et al., *supra* note 88.

306. Thomas Langenfeld, *Internet-Based Proctored Assessment: Security and Fairness Issues*, 39 EDUC. MEASUREMENT, ISSUES & PRAC. 24, 25 (2020).

307. General Data Protection Regulation, *supra* note 295, at art. 22; Colonna, *supra* note 88, at 31.

308. Maples, *supra* note 40.

technologies have on society should be contemplated and freely debated. Criteria specifically mapped for AI technologies based on pedagogical research and vendor claims should be systematically and rigorously verified.[309] The use of synthetic data[310] should also be explored when considering how to improve AIPS algorithms, particularly because the types of data needed (e.g., children's faces) may be more difficult to obtain.[311] By bringing student voices into policy creation, students will have input on how their rights are protected or infringed.

One critique of the GDPR is that the language used is ambiguous and does not provide complainants with a legally mandated right to an explanation of an automated decision.[312] To avoid this, legislators should make explicit the right to an explanation, with clear requirements around what kind of information needs to be furnished by the AI vendor, what qualifies as a decision based solely on automated processing, and what constitutes a "significant effect" of an automated decision.[313] If this is deemed too broad—and AIPS companies argue that it will stifle innovation by reducing companies' incentives to create and improve upon AIPS technologies—a policy more akin to article 20 in Brazil's General Data Protection Law ("LGPD")[314] could be implemented as an alternative. Under article 20, a data subject has the right to request the national authority to review a decision that is solely based on automated processing if that decision affects the subject's interests.[315]

A potential pitfall is that transparency will allow vendors to collude with each other.[316] Other scholars argue that transparency is not enough, and that computer scientists must build in accountability procedures like persistent testing and oversight from technical experts acting as "special masters."[317] However, a group of scholars has developed a game theory model that shows that despite concerns of negative downstream effects, companies are better off

309. MIAO ET AL., *supra* note 6, at 37.

310. Woodie, *supra* note 92.

311. Hye-Min Won, Hyeogjin Lee, Gyuwon Song, Yeonghun Kim & Nojun Kwak, *Reliable Data Collection Methodology for Face Recognition in Preschool Children*, 22 SENSORS (BASEL) 5842, 5842, 5845–46 (2022).

312. Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIV. L. 76, 76–77, 97 (2017).

313. *Id.* at 96–99.

314. *See Brazilian General Data Protection Law (LGPD, English translation)*, IAPP, https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/ (Oct. 2020).

315. *Id.*

316. Thomas Bourveau, Guoman She & Alminas Žaldokas, *Corporate Disclosure as a Tacit Coordination Mechanism: Evidence from Cartel Enforcement Regulations*, 58 J. ACCT. RSCH. 295, 296 (2020); Kroll et al., *supra* note 144, at 633.

317. Kroll et al., *supra* note 144, at 703.

sticking to a policy of transparency rather than keeping their algorithms opaque.[318]

2. Prong 2: Checklist for Educators: A School-Centered Approach

The new educational privacy right would hold schools to a heightened standard where the first thing examined would be the legitimate interests of the institution in adopting AIPS. A school would need to show a compelling reason why the use of AIPS is necessary, and how the service is narrowly tailored to minimize student risk. Because K-12 school attendance is compulsory, students are not voluntarily generating data and therefore deserve greater protection. Educational institutions would need to comprehensively document the balancing test between their interests and students' rights to privacy and data security. When students are able to opt in to a solution with no material difference in their educational experience, the higher educational privacy standard need not be met. To meet this new privacy standard, schools will likely pass the onus onto AIPS vendors, pressuring them to embed privacy-by-design standards into practice.[319]

Even without a new educational privacy right, schools should carefully consider the reputational risks associated with the adoption of AIPS. If the FTC does decide to investigate and finds negligence or wrongdoing, there will be consequences for adverse findings. Schools should also be prepared for pushback from the student body, as some universities experienced during the pandemic.[320] Researchers also encourage educators to think about the incentives these systems create for the students who are evaluated by them.[321] A University of California, Berkeley working group tasked with evaluating remote proctoring in response to ethical concerns recommends that schools first "[d]evelop a vetting process for AI-enabled tools that affect students."[322] The group advises that the use of AIPS "may be preferable to the status quo if it introduces efficiencies" into the assessment experience and simultaneously reduces human bias.[323] This vetting process should include students in order to create a culture

318. Qiaochu Wang, Yan Huang, Stefanus Jasin & Param Vir Singh, Algorithmic Transparency with Strategic Users 25–28 (July 15, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3652656.

319. Archambault, *supra* note 227, at 43.

320. *See* Jason Kelley & Tracy Zhang, *Students Are Pushing Back Against Proctoring Surveillance Apps*, ELEC. FRONTIER FOUND. (Sept. 25, 2020), https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps.

321. Raso et al., *supra* note 55, at 50.

322. UNIV. OF CAL. PRESIDENTIAL WORKING GRP. ON AI, RESPONSIBLE ARTIFICIAL INTELLIGENCE: RECOMMENDATIONS TO GUIDE THE UNIVERSITY OF CALIFORNIA'S ARTIFICIAL INTELLIGENCE STRATEGY FINAL REPORT 61 (2021), https://www.ucop.edu/ethics-compliance-audit-services/compliance/uc-ai-working-group-final-report.pdf.

323. *Id.*

of collaboration and trust that empowers students to feel that they have autonomy and responsibility over their own learning.

The first items to tackle from a school's perspective are operational and technical questions. Schools should ask AIPS vendors for copies of their privacy and data security policies. If the vendor does not have one, the vendor should immediately be eliminated from consideration. If the policies are provided, IT or EdTech professionals should review them to ensure that they address the issues of fairness, accessibility or performance, accountability and transparency, privacy, respect for autonomy, and data security discussed in Part II.[324] Schools should also ask vendors questions on how the software was developed. Were multidisciplinary teams used? Were experts in K-12 pedagogy consulted? Was there legal product counsel involved? Solutions should be proportional to the issues schools are trying to solve. Having privacy and security specialists review contracts, terms of service, and data retention and use policies is ideal. This way, schools ensure proper vetting of tools and have experts on staff who can create and publish privacy policies for various school stakeholders.

Second, to foster meaningful transparency and accountability, schools should encourage dialogue with both students and parents about the use of AIPS and seek affirmative consent for their use. This means that students and parents should be notified that their school is implementing AIPS and should then be able to opt in rather than out of its use. There should not be any meaningful difference in the student's overall educational experience regardless of which option they choose. There should also be a line of open communication between school decisionmakers, parents, and students so that all sides can raise concerns as well as take active part in making recommendations. Technology policies should be iterative, requiring ongoing recalibration and feedback to get right.[325] Additionally, having a well-crafted data governance policy will assist schools in making data usage to parents and students more transparent. Student and privacy rights groups also recommend that schools include in their policy a commitment to share only the minimum amount of personal information with vendors and authorities, and only for specific, narrowly tailored, and documented purposes.[326] Professional development on student privacy should also be required for all relevant faculty and staff.

CONCLUSION

There are clear ethical concerns around the usage of AIPS that are especially magnified for school-aged children. The potential negative effects are

---

324. *See supra* Part II.

325. Fedders, *supra* note 84, at 1724.

326. *Education During a Pandemic: Principles for Student Data Privacy and Equity*, STUDENT PRIV. COMPASS (Oct. 27, 2020), https://studentprivacycompass.org/pandemicprinciples/.

significant given the unique time in a young person's life when AIPS are introduced. Therefore, AIPS should be implemented only after careful consideration, if at all. The creation of an educational privacy right would facilitate this inquiry by providing institutions with guidelines on how to analyze the liability risk of AIPS adoption against the benefits they would afford, while also providing protections through federal regulation of private industry.

Further research into the efficacy of AI proctoring systems would be helpful to determine whether the systems are promoting rather than dispelling academic misconduct, whether the systems are effective at preventing and detecting cheating, and whether the evidence generated is useful in navigating the disciplinary process with students. Large-scale evaluations of all AI systems should be conducted, considering appropriateness for the local region and context. In the meantime, a variety of proven analog alternatives exist to ensure that academic integrity is preserved and students continue to learn despite external variables.

* * *