Notre Dame Journal on Emerging Technologies

Volume 3
Issue 1 *Artificial Intelligence*

Article 3

2-2022

Big Proctor: Online Proctoring Problems and How FERPA Can Promote Student Data Due Process

Elana Zeide
University of Nebraska College of Law

Big Proctor: Online Proctoring Problems and How FERPA Can Promote Student Data Due Process

Erratum

The editors recognize that the header date for the article is January 2023, which reflects the date final editing occurred.

Volume 3 January 2023 Issue 1

JOURNAL ON EMERGING TECHNOLOGIES

ARTICLES

BIG PROCTOR: ONLINE PROCTORING PROBLEMS AND HOW FERPA CAN PROMOTE STUDENT DATA DUE PROCESS

Elana Zeide

When the pandemic forced schools to shift to remote education, school administrators worried that unsupervised exams would lead to widespread cheating. Many turned to online proctoring technologies that use facial recognition, algorithmic profiling, and invasive surveillance to detect and deter academic misconduct. It was an "epic fail."[1]

Intrusive and unproven remote proctoring systems were inaccurate, unfair—and often ineffectual. The software did not account for foreseeable student diversity, leading to misidentification and false flags that disadvantaged test-takers from marginalized communities. Educators implemented proctoring software without sufficient transparency, training, and oversight. As a result, students suffered privacy, academic, reputational, pedagogical, and psychological harms.

Online proctoring problems prompted significant public backlash but no systemic reform. Students have little recourse under existing legal frameworks, including current biometric privacy, consumer protection, and antidiscrimination laws. Student privacy laws like the Family Educational Rights and Privacy Act (FERPA) also offer minimal protection against schools' education technology. However, FERPA's overlooked rights of review, explanation, and contestation offer a stopgap solution to promote algorithmic accountability and due process.

---

[1] Credit for this phrase goes to Marsha Griggs, *An Epic Fail*, 64 HOWARD L.J. 1 (2020).

The article recommends a moratorium on online proctoring technologies until companies can demonstrate that they are accurate and fair. It also calls for schools to reject software that relies on prolonged surveillance and pseudoscientific automated profiling. Finally, it recommends technical, institutional, and pedagogical measures to mitigate proctoring problems in the absence of systemic reform.

BIG PROCTOR: ONLINE PROCTORING PROBLEMS AND HOW FERPA CAN PROMOTE STUDENT DATA DUE PROCESS

Elana Zeide[2]

INTRODUCTION

It's every student's worst nightmare: you've studied hard for an exam and are about to wrap up a tough essay. Suddenly, you get locked out of the test—the proctoring software flagged your rifling through notes as suspicious. When tech support finally manages to get you back in the system, your essay is gone, along with most of your time to complete the test. Or maybe you've finished the test and are feeling confident. But because you've looked away from the screen, lost in thought, your professor won't give you credit unless the dean determines you're not guilty of cheating.

These scenarios are all too real for many test-takers who took the bar exam online in 2020 and 2021. Students worldwide faced similar problems when schools administered tests through online platforms accompanied by remote proctoring software. Online proctoring technology (OPT) vendors promised that extensive surveillance, facial recognition, and algorithmic profiling would prevent and detect cheating.[3] They became ubiquitous, especially in U.S. higher education

---

[2] Assistant Professor, University of Nebraska College of Law; Fellow, Silicon Flatirons, University of Colorado-Boulder; Affiliate Fellow, Yale Law School Information Society Project. Many thanks to Gus Hurwitz, Kyle Langvardt, Brenda Leong, Amelia Vance, Abagail Jacobs, Bobby Truhe, Lauren Brown, McKinley Brock, and Emma Schlenker for their attention and suggestions and to the devoted editors of the *Notre Dame Journal on Emerging Technologies*.

[3] S. Decker et al., *The Coronavirus Spring: The Historic Closing of US Schools (A Timeline)*, EDWEEK (July 1, 2020), https://www.edweek.org/leadership/the-coronavirus-spring-the-historic-closing-of-u-s-schools-a-timeline/2020/07; Raghu Raman et al., *Adoption of Online Proctored Examinations by University Students during COVID-19: Innovation Diffusion Study*, 26 EDUC. INFO. TECH. 7339 (2021); 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; Jeffrey Young, *Automated Proctoring Swept In During Pandemic. It's Likely to Stick Around, Despite Concerns*, EDSURGE (Nov. 19, 2021), https://www.edsurge.com/news/2021-11-19-automated-proctoring-swept-in-during-pandemic-it-s-likely-to-stick-around-despite-concerns; Neil Selwyn et al., *A Necessary Evil? The Rise of Online Exam Proctoring in Australian Universities*, 186 MEDIA INT'L AUSTR. 149 (2023).

institutions.[4] However, many automated proctoring technologies proved inaccurate, unfair, and invasive–and were not even effective at spotting academic misconduct.

Online proctoring has become part of the new normal.[5] However, current legal regimes don't address the harms inflicted by proctoring technologies.[6] Privacy, consumer protection, and antidiscrimination laws offer aggrieved test-takers minimal recourse. They also place negligible pressure on vendors to improve their technologies and on schools to implement better institutional practices.[7]

This article offers a systemic analysis of the technical, institutional, and pedagogical problems posed by proctoring technologies.[8] It then disambiguates the components of proctoring technologies, considering their design, features, and computing processes, as well as their implementation by schools and teachers.[9] Most online proctoring services rely on controversial technologies—facial recognition, artificial intelligence, and biometric surveillance.[10]

---

[4] Royce Kimmons & George Velestsianos, *Proctoring Software in Higher Ed: Prevalence and Patterns*, EDUCAUSE (Feb. 23, 2021), https://er.educause.edu/articles/2021/2/proctoring-software-in-higher-ed-prevalence-and-patterns (finding 65.8% of U.S. university websites mention one of the five top proctoring service providers).

[5] *See, e.g.*, *The Worldwide Online Exam Proctoring Industry is Projected to Reach $1.5 Billion by 2028*, BUS. WIRE (June 23, 2022, 8:14 AM), https://www.businesswire.com/news/home/20220623005577/en/The-Worldwide-Online-Exam-Proctoring-Industry-is-Projected-to-Reach-1.5-Billion-by-2028---ResearchAndMarkets.com.

[6] *See, infra*, Part II.

[7] As this article was in the final stages of production, a federal court ruled that a ten-second video scan of a student's room before a test was an unreasonable search in violation of the Fourth Amendment. s No. 21-CV-00500, 2022 WL 17826730 (N.D. Ohio Dec. 20, 2022). The court found the university did not meet the "special needs" exception that would justify a suspicionless search, noting that the minimally intrusive nature of the scan and the school's legitimate interest in preserving the integrity of remote tests were outweighed by the student's significant privacy interest in his bedroom and undermined by the lack of evidence supporting the efficacy of rooms scans in preventing cheating. *Id.* at 18-23. However, the remote proctoring in *Ogletree* was anomalous—the school used Zoom video conferencing to conduct the scan, which was also visible to the student's classmates. *Id.* at 4. As a result, courts may not come to the same conclusion when considering more typical remote proctoring contexts where only company proctors and educators can view surveillance footage.

[8] *See infra* Part I.

[9] *See infra* Part I.

[10] *See infra* Section I.B.

But neither vendors nor schools accounted for foreseeable problems by ensuring sufficient accuracy, oversight, or avenues for student appeal.[11]

Part I details the deployment of online proctoring systems during the pandemic, the resulting problems, and the extraordinary popular and political pushback. It then disambiguates the relevant components of proctoring technologies, considering their technical features and implementation by schools and teachers. Online proctoring software relies on controversial technologies—facial recognition, artificial intelligence, and biometric surveillance in intimate surroundings. But neither vendors nor schools accounted for their foreseeable flaws by ensuring sufficient accuracy, oversight, or avenues for appeal. In short, pandemic proctoring practices are unacceptable and unjustified.[12]

Part II considers strategies across several legal regimes that might apply to pandemic online proctoring and finds them sorely wanting. Student and biometric privacy, consumer protection, and antidiscrimination law offer aggrieved students minimal recourse and place negligible pressure on vendors and schools to improve their technologies or institutional practices.

Student privacy laws focus primarily on preventing unauthorized disclosure or commercialization of student information, not protecting them against problematic school-approved technologies or surveillance. With sufficient supporting evidence, the Federal Trade Commission (FTC) could find that OPS vendors' overblown and unproven claims constitute deceptive trade practices.[13] More tenuously, the agency could use pandemic proctoring as an opportunity to regulate artificial intelligence more aggressively by finding that vendors' use of artificial intelligence (AI) is an unfair trade practice. Antidiscrimination claims face significant substantive and procedural obstacles.

This article offers a stopgap solution to promote algorithmic due process using FERPA's overlooked rights of inspection, explanation, and contestation.[14] The statute gives students the right to inspect personal information in education records held by schools and vendors—and to challenge information they believe to be inaccurate or inappropriate. To support these rights, the U.S. Department of Education (ED) requires schools and vendors to explain the information in the records. In the context of online proctoring, this could include providing students with raw surveillance footage and the basis for

---

[11] *See infra* Section I.C.
[12] *See also* Simon Coghlan et al., *Good Proctor or "Big Brother"? Ethics of Online Exam Supervision Technologies*, 34 PHIL. & TECH. 1581, 1600 (2021).
[13] *See infra* Section II.B.
[14] *See infra* Section II.A.

algorithm-generated cheating flags and suspicion scores. In light of ED's recent Agora letter, this strategy offers students a means to pursue due process and promote algorithmic accountability without depending on unlikely agency enforcement.[15]

Given the inadequacy and uncertainty of current legal frameworks, Part III proposes a moratorium on proctoring technologies, rejecting their unproven features, and, at the very least, reserving their use only when truly necessary, not just expedient. This article also suggests technical, institutional, and pedagogical reforms to at least improve upon proctoring technologies absent a moratorium. Pandemic proctoring showcases the limits of the student privacy status quo, which allows schools to adopt unproven technologies without sufficient oversight or due process. It offers a cautionary tale that calls for vendors, educators, and policymakers to protect students from problematic education technology.

I. ONLINE PROCTORING SOCIOTECHNICAL SYSTEMS

The pandemic shift to remote learning put education technology in the public spotlight. Before March 2020, students might occasionally complete homework, view learning material, or take tests on a device, but technology used for pedagogical purposes was not a prominent part of their educational experiences.

A. Pandemic Proctoring

Everything changed when schools switched to remote learning during the COVID-19 pandemic.[16] Parents suddenly had to navigate learning management systems and oversee automated lessons; students attended class and took tests remotely; and, of course, everyone had to Zoom, Zoom, and Zoom some more. Schools and professional associations also administered tests through online platforms—and

---

[15] *See infra* Section II.A.4 and 5.
[16] Decker et al., *supra* note 3.

worried about ways to ensure academic integrity in the absence of human supervision.[17]

The speed and extent of pandemic proctoring technology adoption were remarkable.[18] As early as April 2020, a poll found that more than half of the higher education institutions surveyed already had an online proctoring solution, and almost a quarter were "planning or considering using them.[19] Many K–12 schools adopted proctoring technologies after the ED announced it would permit the remote administration of required state assessments.[20] Proctoring technologies became ubiquitous among higher education institutions in North America.[21] The number of schools using three prominent OPTs — ExamSoft, Proctorio, and ProctorU (now rebranded as Meazure Learning)—increased by as much as 500% after the start of the pandemic.[22] These three vendors proctored over 30 million tests as of June 2021.[23]

---

[17] Karen Symms Gallagher, *Op-Ed: Rampant Online Cheating is the Dark Side of Remote Learning*, L.A. TIMES (Oct. 24, 2021), https://www.latimes.com/opinion/story/2021-10-24/online-cheating-apps-remote-learning; Tawnell D. Hobbs, *Cheating at School Is Easier Than Ever—and It's Rampant*, WALL ST. J. (May 12, 2021), https://www.wsj.com/articles/cheating-at-school-is-easier-than-everand-its-rampant-11620828004; Derek Newton, *Another Problem with Shifting Education Online: Cheating*, WASH. POST (Aug. 7, 2020), https://www.washingtonpost.com/local/education/another-problem-with-shifting-education-online-a-rise-in-cheating/2020/08/07/1284c9f6-d762-11ea-aff6-220dd3a14741_story.html; Elizabeth Broadbent, *Online Cheating Is A Big Problem With College Students–Current Solutions Seem Problematic*, SCARY MOMMY (Sept. 14, 2021), https://www.scarymommy.com/online-cheating-rampant-solutions-violate-privacy/; Sneha Dey, *Reports Of Cheating At Colleges Soar During The Pandemic*, NPR (Aug. 27, 2021, 6:00 AM), https://www.npr.org/2021/08/27/1031255390/reports-of-cheating-at-colleges-soar-during-the-pandemic; Seife Dendir & R. Stockton Maxwell, *Cheating in Online Courses: Evidence from Online Proctoring*, 2 COMPUTS. HUM. BEHAV. REPS. 100033 (2020).

[18] Decker et al., *supra* note 3; Raman et al., *supra* note 3; Caplan-Bricker, *supra* note 3; Young, *supra* note 3; Selwyn et al., *supra* note 3.

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

[20] Letter from U.S. Dep't Of. of Elementary and Secondary Educ. to Chief State School Officers (Feb. 22, 2021), https://oese.ed.gov/files/2021/02/DCL-on-assessments-and-acct-final.pdf.

[21] Kimmons & Velestsianos, *supra* note 4; Raman et al., *supra* note 3.

[22] Caplan-Bricker, *supra* note 3.

[23] This statistic includes professional licensing tests administered by professional associations, most notably state bar exams. Jason Kelley, *A Long Overdue Reckoning For Online Proctoring Companies May Finally Be Here*, ELEC. FRONTIER FOUND. (June 22, 2021), https://www.eff.org/deeplinks/2021/06/long-overdue-reckoning-online-proctoring-companies-may-finally-be-here.

Horror stories quickly surfaced online.[24] Automated cheating detection systems flagged innocuous behavior as "suspicious" without explanation.[25] One student could not take a test because the testing

---

[24] Tony Wan, *Automated Proctors Watch Students. Now Senators Are Watching These Companies*, EDSURGE (Dec. 8, 2020), https://www.edsurge.com/news/2020-12-08-automated-proctors-watch-students-now-senators-are-watching-these-companies; Jack Morse, *Online Testing is a Biased Mess, and Senators Are Demanding Answers*, MASHABLE (Dec. 3, 2020), https://mashable.com/article/senate-open-letter-remote-proctoring-examsoft-bias-student-privacy/; Avi Asher-Schapiro, *Online Exams Raise Concerns of Racial Bias in Facial Recognition*, CHRISTIAN SCI. MONITOR (Nov. 17, 2020), https://www.csmonitor.com/Technology/2020/1117/Online-exams-raise-concerns-of-racial-bias-in-facial-recognition; Avi Asher-Schapiro, *"Unfair Surveillance"? Online Exam Software Sparks Global Student Revolt*, REUTERS (Nov. 10, 2020, 7:24 AM), https://www.reuters.com/article/global-tech-education-idUSL8N2HP5DS; 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/ [hereinafter *Cheating-Detection Companies*]; Jane C. Hu, *Online Test Proctoring Claims to Prevent Cheating. But at What Cost?*, SLATE MAG. (Oct. 26, 2020, 9:00 AM), https://slate.com/technology/2020/10/online-proctoring-proctoru-proctorio-cheating-research.html; 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), https://www.insider.com/viral-tiktok-student-fails-exam-after-ai-software-flags-cheating-2020-10; 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; Drew Harwell, *Mass School Closures in the Wake of the Coronavirus Are Driving a New Wave of Student Surveillance*, WASH. POST (Apr. 1, 2020), https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/ [hereinafter *Mass School Closures*].

[25] Patil & Bromwich, *supra* note 24; *Mass School Closures*, *supra* note 24; Monica Chin, *Exam Anxiety: How Remote Test-Proctoring is Creeping Students Out*, THE VERGE (Apr. 29, 2020), https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education; 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; Albert Fox Cahn et al., *Snooping Where We Sleep: The Invasiveness and Bias of Remote Proctoring Services*, SURVEILLANCE TECH. OVERSIGHT PROJECT (Nov. 11, 2020), https://www.stopspying.org/snooping; Evan Selinger, *Abolish A.I. Proctoring: Evan Selinger in Conversation with Chris Gilliard*, MEDIUM (Apr. 7, 2021), https://onezero.medium.com/abolish-a-i-proctoring-c9e017dd764f.; Jason Kelley et al., *Proctoring Tools and Dragnet Investigations Rob Students of Due Process*, ELECTRONIC FRONTIER FOUND. (Apr. 15, 2021), https://www.eff.org/deeplinks/2021/04/proctoring-tools-and-dragnet-

software did not recognize his dark skin and could not confirm his identity.[26] Software flagged another student for thinking aloud.[27] Other students had their scores invalidated for looking at their calculators instead of the screen.[28] Students might be locked out of exams if the software sensed a pop-up notification[29] or poor internet connection.[30]

Students, parents, educators, and advocacy groups responded with appropriate outrage.[31] These problems prompted widespread backlash, with commentators critiquing proctoring technologies as invasive, discriminatory, ineffective, and unnecessary.[32] Students, parents, and teachers signed petitions and pressured schools to stop using online proctoring tools.[33] Over 19 human rights, civil liberties,

---

investigations-rob-students-due-process; Shea Swauger, *Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education*, HYBRID PEDAGOGY (Apr. 2, 2020), https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/; Lindsey Barrett, *Rejecting Test Surveillance in Higher Education*, 2022 MICH. ST. L. REV. 775 (2022); *Protect Student Privacy: Ban Eproctoring*, FIGHT FOR THE FUTURE, https://www.baneproctoring.com/.

[26] Kelly Meyerhofer, *3 UW-Madison Students Say Online Exam Software Didn't Detect Their Darker Skin*, WIS. STATE J. (Apr. 5, 2021), https://madison.com/news/local/education/university/3-uw-madison-students-say-online-exam-software-didnt-detect-their-darker-skin/article_891b3e5a-a9e3-5529-8859-e20908dee0b6.html; Todd Feathers, *Proctorio Is Using Racist Algorithms to Detect Faces*, VICE (Apr. 8, 2021, 12:48 PM), https://www.vice.com/en/article/g5gxg3/proctorio-is-using-racist-algorithms-to-detect-faces; Joe Patrice, *Online Bar Exams Rely On Facial Recognition Tech And Guess What? It's Still Racist!*, ABOVE THE LAW (Sept. 18, 2020, 12:32 PM), https://abovethelaw.com/2020/09/online-bar-exams-rely-on-facial-recognition-tech-and-guess-what-its-still-racist/.

[27] Harris, *supra* note 24.

[28] Carl T. Bergstrom (@CT_Bergstrom), TWITTER (Oct. 30, 2020, 10:46 PM), https://twitter.com/CT_Bergstrom/status/1322369360552357888.

[29] Yassie Buchanan, *Opinion: Online Proctoring Harms More than Helps*, THE DAILY IOWAN (Feb. 18, 2021), https://dailyiowan.com/2021/02/18/opinion-online-proctoring-harms-more-than-helps/.

[30] Shea Swauger, *Remote Testing Monitored by AI is Failing the Students Forced to Undergo It*, NBC NEWS (Nov. 7, 2020, 4:30 AM), https://www.nbcnews.com/think/opinion/remote-testing-monitored-ai-failing-students-forced-undergo-it-ncna1246769.

[31] Cahn et al., *supra* note 25; Selinger, *supra* note 25.

[32] *Id.*

[33] *See, e.g.*, Todd Feathers & Janus Rose, *Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools,* VICE (Sept. 24, 2020, 6:00 AM), https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools; Jason Kelley, *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-

and youth advocacy organizations called for school administrators to ban proctoring software.[34] Students in Illinois sued proctoring technology providers and private schools for violating Illinois' Biometric Information Privacy Act (BIPA).[35] The Electronic Privacy Information Center filed a complaint with the Attorney General of the District of Columbia, alleging that vendors engaged in unfair and deceptive trade practices.[36] Several U.S. senators wrote to proctoring vendors expressing concern and requesting information about the efficacy and impact of their software.[37]

---

proctoring-surveillance-apps; *Mass School Closures*, *supra* note 24; *2000 Parents Call on McGraw-Hill Publishing to End Partnership with Proctorio*, FIGHT FOR THE FUTURE (Dec. 17, 2020), https://www.fightforthefuture.org/news/2020-12-17-2000-parents-call-on-mcgraw-hill-publishing-to-end/; Madeline Thompson, *UCSB Faculty Association Issues Letter Advising Against the Use of ProctorU Testing Services,* DAILY NEXUS (Mar. 16, 2020), https://dailynexus.com/2020-03-16/ucsb-faculty- association-issues-letter-advising-against-the-use-of-proctoru-testing-services/; Mark Mussachio, *The "New" (and Deeply Dissatisfied) Users of Online Proctoring*, ONLINE LEARNING CONSORTIUM (Dec. 15, 2020), https://onlinelearningconsortium.org/the-new-and-deeply-dissatisfied-users-of-online-proctoring/. *See, e.g.*, *Protect Student Privacy: Ban Eproctoring*, *supra* note 25 (listing higher education institutions using e-proctoring tools).

[34] *See, e.g.*, Feathers & Rose, *supra* note 33; Kelley, *supra* note 33; *Mass School Closures*, *supra* note 24; *2000 Parents Call on McGraw-Hill Publishing to End Partnership with Proctorio*, *supra* note 33; Thompson, *supra* note 33; Mussachio, *supra* note 33; *Protect Student Privacy: Ban Eproctoring*, *supra* note 25; Morgan Lavaway, *Ban Online Proctoring at University of Washington Tacoma (Proctoring, Not Online Testing)*, CHANGE.ORG, https://www.change.org/p/university-of-washington-tacoma-students-and-faculty-ban-online-proctoring-at; Kari Paul, *"Ban this Technology": Students Protest US Universities' Use of Facial Recognition*, THE GUARDIAN (Mar. 2, 2020), https://www.theguardian.com/us-news/2020/mar/02/facial-recognition-us-colleges-ucla-ban; Selinger, *supra* note 25.

[35] 740 ILL. COMP. STAT. §§ 14, 15 (2022).

[36] Complaint, In the Matter of Online Test Proctoring Companies Respondus, Inc.; ProctorU, Inc.; Proctorio, Inc.; Examity, Inc., and Honorlock, Inc. (Dec. 2020), https://epic.org/wp-content/uploads/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf [hereinafter *Complaint and Request for Investigation*]; D.C. CONSUMER PROTECTION PROCEDURES ACT, D.C. CODE §§ 28-3904, 28-3904(e), and 28-3904(f); Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

[37] Letter from Sen. Richard Blumenthal et al. to Sabastian Vos, Chief Exec. Officer, ExamSoft, at 2 (Dec. 3, 2020), https://www.blumenthal.senate.gov/imo/media/doc/2020.12.3%20Letter%20to%20Ed%20Testing %20Software%20Companies%20ExamSoft.pdf.

Some schools did reject or reduce their use of proctoring technology in response.[38] Vendors disclaimed responsibility—saying that their clients chose what services to use, determined what flagging parameters to set, and decided whether students' behavior indicated academic misconduct.[39] One prominent provider, ProctorU, admitted that fully automated proctoring "doesn't work" and stopped offering services without human review.[40] Another provider, Proctorio, engaged a bias research consultant to improve its facial detection algorithm (but not its cheating detection tools).[41] Many vendors simply toned down their marketing promises or updated product descriptions to clarify, for example, that they use "face and gaze detection" rather than "facial recognition."[42] But there was no systemic reform. Years later, most students are still at the mercy of proctoring technologies—no matter how poorly designed, hastily implemented, or pedagogically unsound. And now it is clear that online proctoring will not end with the pandemic.[43]

---

[38] Natalie Schwarz, *Colleges Flock to Online Proctors, But Equity Concerns Remain*, HIGHER ED DIVE (Apr. 7, 2020), https://www.highereddive.com/news/colleges-flock-to-online-proctors-but-equity-concerns-remain/575642/ (describing U.C. Davis' discouragement of remote proctoring unless faculty has prior experience); *Protect Student Privacy: Ban Eproctoring*, *supra* note 25.

[39] *See, e.g.*, Letter from Mike Olsen, Founder/CEO, Proctorio, Inc., to Sen. Richard Blumenthal et al. (Jan. 7, 2021), EPIC, https://epic.org/wp-content/uploads/privacy/dccppa/online-test-proctoring/Proctorio-senate-response-010721.pdf; Letter from Sabastian Vos, Chief Exec. Officer, ExamSoft, letter to Sen. Richard Blumenthal et al., (Dec. 17, 2020) https://docs.google.com/viewerng/viewer?url=https://abovethelaw.com/uploads/2021/01/ExamSoft-letter.pdf&hl=en_US ("Ultimately the exam-taker's institution will make the decision on any anomalies flagged by the software.").

[40] Scott MacFarland, *AI-Only Proctoring is Risky and Doesn't Work. We're Not Doing It Any More*, TIMES HIGHER EDUC. (May 29, 2021), https://www.timeshighereducation.com/blog/ai-only-proctoring-risky-and-doesnt-work-were-not-doing-it-any-more; Kelley, *supra* note 23.

[41] Mike Olsen, *Proctorio Addresses Remote Proctoring Industry Concerns*, PROCTORIO (Aug. 24, 2021), https://proctorio.com/about/blog/proctorio-addresses-remote-proctoring-industry-concerns/.

[42] *See, e.g.*, *Proctorio Misconceptions FAQ,* USI (Oct. 2020), https://www.usi.edu/media/5629942/misconceptions-faq.pdf; *Face Detection vs Face Recognition in Online Proctoring*, HONORLOCK (Oct. 29, 2021), https://honorlock.com/blog/face-detection-vs-face-recognition-in-online-proctoring/.

[43] Caplan-Bricker, *supra* note 3; Young, *supra* note 3; Selwyn et al., *supra* note 3; *The Worldwide Online Exam Proctoring Industry is Projected to Reach $1.5 Billion by 2028*, *supra* note 5.

B. Proctoring Technology Problems

While the use of online proctoring software surged with the pandemic in 2020, this technology is not new. Schools have been using versions of online proctoring tools to administer online exams for over a decade.[44] OPT vendors have long tried to replicate the functions of in-person proctors: they use remote human employees and technology to verify test-takers' identities, limit access to prohibited materials, and "monitor" test-takers to discourage and detect cheating.[45]

Students typically install some proctoring software on their devices. The software then verifies the exam-taker's identity.[46] Then, lockdown components disable browsing and navigation and capture features on students' devices to prevent them from looking up answers or saving test questions.[47] Schools can choose from three monitoring modalities: real-time human proctoring, automated proctoring, and automated proctoring plus human review.[48]

With real-time human proctoring, vendor-trained proctors observe one or more test-takers through video-conferencing technologies.[49] They may watch students continuously or "pop in" if an automated system detects suspicious activity.[50] OPTs' monitoring systems record and analyze students' digital behavior, physical activity, and testing environment.[51] Automated proctoring technologies use artificial intelligence to identify when a test-taker engages in suspicious behavior.[52]

The software generates a report for educators that includes a timeline of student activity (such as when students answer questions,

---

[44] Tony Wan, *As Online Learning Grows, So Will Proctors. Case in Point: Examity's $90M Deal*, EDSURGE (Apr. 30, 2019), https://www.edsurge.com/news/2019-04-30-as-online-learning-grows-so-will-remote-proctors-case-in-point-examity-s-90m-deal.
[45] *See* INT'L PRIVACY SUBCOMM. OF THE ATP SECURITY COMM., ASS'N OF TEST PUBLISHERS SEC. COMM., ARTIFICIAL INTELLIGENCE AND THE TESTING INDUSTRY: A PRIMER at 8 (2021), https://www.testpublishers.org/assets/ATP%20White%20Paper_AI%20and%20Testing_A%20Primer_6July2021_Final%20R1%20.pdf
[46] *A.I. Proctoring: Invigilation Exam Day Guide*, EXAMSOFT (May 26, 2021), https://examsoft.com/resources/proctoring-invigilation-exam-day-guide.
[47] Simone Arnò et al., *State-of-the-Art of Commercial Proctoring Systems and Their Use in Academic Online Exams*, 19 INT'L J. DISTANCE EDUC. TECH. 55, 58 (2021).
[48] *Id.* at 56.
[49] *Id.* at 58.
[50] *Id.*
[51] *Id.*
[52] *Id.*

their internet service disconnects, or multiple faces appear in the video frame).[53] Vendors also tabulate "Suspicion Score[s]";[54] Proctorio, for example, places suspicion scores on a red, yellow, and green scale to suggest which exams need review.[55] Vendors also provide aggregated class data, including the average time users spent on a question and to complete the entire exam.[56] Automated proctoring "plus" services have a vendor-employed proctor review the report for an additional fee.[57]

OPTs boast that their automated systems spot indicators of cheating that humans miss.[58] Several providers also claim that artificial intelligence reduces bias.[59] However, anecdotal evidence, vendors' own statements, and emerging research suggest that proctoring technology doesn't deliver on its promises—and is, in fact, counterproductive.

OPTs are unreliable, inaccurate, and unfair.[60] Vendors employ flawed facial verification, biased and unproven algorithmic profiling, and intrusive biometric surveillance to deter cheating.[61] These features, however, may be no more effective than a placebo.[62] At the same time, proctoring systems inflict privacy, academic, reputational, pedagogical,

---

[53] *Additional Privacy Information - Respondus Monitor*, RESPONDUS (2022), https://web.respondus.com/privacy/privacy-additional-monitor/; *Automated or Live Online Proctoring*, PROCTORIO, https://proctorio.com/products/online-proctoring (last accessed Mar. 1, 2022).

[54] *Id.*

[55] *Automated or Live Online Proctoring*, *supra* note 53.

[56] *See, e.g.*, *id.*

[57] *See, e.g.*, *id.*

[58] *Artificial Intelligence in Online Proctoring: Where We've Been, Where We Are, and Where We're Going*, PROCTORU (Sept. 10, 2018), https://www.proctoru.com/industry-news-and-notes/artificial-intelligence-in-online-proctoring-where-weve-been-where-we-are-and-where-were-going ("ProctorU's goal in introducing AI into proctoring is not to replace humans but, rather, to strengthen the accuracy of proctoring by assisting humans in identifying details such as shadows, whispers or low sound levels, reflections, etc., that may otherwise go unnoticed.").

[59] *See, e.g.*, Coghlan et al., *supra* note 12, at 1592 ("[Proctoring] [c]ompanies claim that well-designed AI can also mitigate human bias and error"); *Platform*, PROCTORIO (2020), https://proctorio.com/platform. *See, e.g.*, PROCTORIO, https://web.archive.org/web/20210430212733/https://proctorio.com/ ("Our software attempts to remove human bias and error.") (last accessed June 24, 2021); Proctorio (@Proctorio), TWITTER, (Jan. 9, 2019 10:04 AM), screenshot available at Ian Linkletter (@Linkletter), TWITTER (Nov. 5, 2020 4:47 PM) (stating "Proctorio is the first and only proctoring solution that combines facial recognition technology and machine learning to eliminate any human error or bias. We utilize this technology to protect academic integrity, and expand learning opportunities globally. #EdTech") (last accessed June 24, 2021).

[60] *See infra* Section I.B.

[61] *See infra* Section I.B.1–3.

[62] *See infra* Section I.B.4.

and psychological harms.[63] Ad hoc school implementation without sufficient accountability or due process exacerbates these problems.[64]

Public data regarding OPTs' accuracy, efficacy, and implementation is scant; while vendors may share information with customers upon request,[65] they have not been forthcoming with evidence supporting their products' performance.[66] In fact, some OPTs have responded to criticism by simply deleting accuracy claims.[67] One notable exception is ProctorU, which shared alarming statistics about the potential for its automated systems to flag innocent behavior when it announced that it would no longer offer AI-only proctoring.[68] Researchers are only beginning to fill this data void.[69] Even if OPTs turn

---

[63] For an account of different kinds of privacy harms, see Danielle Citron & Daniel Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022).

[64] *See infra* Section I.C.

[65] Olsen, *supra* note 41.

[66] *See* Coghlan et al., *supra* note 12, at 1593 ("[T]he operation of [OPS AI] systems is often opaque, and although claims are made about accuracy, the OP company websites rarely if ever cite rigorous studies to justify their claims and to eliminate concerns about false positives . . . ."). Some students performed their own small-scale experiments testing various proctoring suites. *See, e.g.*, Akash Satheesan, *Proctorio's Facial Recognition Is Racist*, PROCTOR NINJA (Mar. 18, 2021), https://proctor.ninja/proctorios-facial-recognition-is-racist. Teachers have shared examples of proctoring technology problems. *See, e.g.*, UC Santa Barbara Faculty Association, *Letter from UC Santa Barbara Faculty Re: Proctoring,* COUNCIL OF UC FAC. ASS'NS (Mar. 13, 2020), https://cucfa.org/wp-content/uploads/2020/03/ProctorU_2020-1.pdf.

[67] In 2019, one remote proctoring employee described its technology as an "[i]ncredibly futuristic AI Algorithm that auto-flags a variety of suspicious cases with 95%+ accuracy." Romila Kanchan, *Top 7 Remote Proctoring Software and Service Providers*, METTL (Feb. 20, 2019), https://blog.mettl.com/proctoring-services-and-solution/ (last accessed July 24, 2021) (as originally published in 2019; updated in 2022 to remove the sentence claiming 95% accuracy). The assertion of a specific accuracy threshold disappeared in early 2022.

[68] MacFarland, *supra* note 40.

[69] *See, e.g.*, Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, 20 PSYCH. SCI. PUB. INT. 1 (2019); Ben Burgess et al., *Watching the Watchers: Bias and Vulnerability in Remote Proctoring Software*, 31 USENIX SEC. SYMP. 571 (2022); Coghlan et al., *supra* note 12; Liane Colonna, *Legal Implications of Using AI as an Exam Invigilator*, (Stockholm Fac. of L. Rsch. Paper Series, Paper No. 91, 2021), https://ssrn.com/abstract=3839287; Thomas Langenfeld, *Internet-Based Proctored Assessment: Security and Fairness Issues*, 39 EDUC. MEASUREMENT: ISSUES AND PRAC.

out to be more accurate than current evidence suggest, the use of unproven and harmful technology without sufficient oversight is problematic in and of itself.

1. Flawed Facial Verification

Until the widespread deployment of remote proctoring, the most prominent school use of facial recognition was to match faces on school premises to a database of students, parents, and staff to detect unauthorized visitors.[70] Facial recognition technology has been criticized as inaccurate, ineffectual, and liable to disproportionately target students of color.[71] They also raise concerns about normalizing surveillance and exposing children's biometric data to security risks.[72] After strident pushback, many schools and states have rejected or paused the implementation of facial recognition security systems.[73] New York, for example, has prohibited schools from purchasing biometric

---

24 (2020); Leah A. Plunkett & Michael S. Lewis, *Education Contracts of Adhesion in the COVID-19 Pandemic*, 2021 U. ILL. L. REV. ONLINE 1 (2021); Selwyn et al., *supra* note 3; Sarah Silverman et al., *What Happens When You Close the Door on Remote Proctoring? Moving Toward Authentic Assessments with a People-Centered Approach*, 39 IMPROVE ACAD.: J. EDUC. DEV. 115 (2021).

[70] *See, e.g.*, Shuran Zhao, *Facial Recognition in Educational Context*, 586 ADVANCES SOC. SCI., EDUC. & HUMS. RSCH. 10, 13–14 (2021); Mark Andrejevic & Neil Selwyn, *Facial Recognition Technology in Schools: Critical Questions and Concerns*, 45 LEARNING, MEDIA & TECH. 115, 122–23 (2020); CLAIRE GALLIGAN ET AL., CAMERAS IN THE CLASSROOM: FACIAL RECOGNITION TECHNOLOGY IN SCHOOLS (2020), https://stppstage.fordschool.umich.edu/sites/stpp/files/2021-07/cameras_in_the_classroom_full_report.pdf; Stefanie Coyle & John A. Curr III, *Facial Recognition Cameras Do Not Belong in Schools*, N.Y. CIV. LIBERTIES UNION (June 18, 2018), https://www.nyclu.org/en/news/facial-recognition-cameras-do-not-belong-schools; Lotem Perry Hazan, *The Hidden Human Rights Curriculum of Surveillance Cameras in Schools: Due Process, Privacy and Trust*, 48 CAMBRIDGE J. EDUC. 47, 50–51 (2016).

[71] *See, e.g.*, Zhao, *supra* note 70; Andrejevic & Selwyn, *supra* note 70; GALLIGAN ET AL., *supra* note 70; Coyle & Curr, *supra* note 70; Hazan, *supra* note 70.

[72] *See, e.g.*, Zhao, *supra* note 70; Andrejevic & Selwyn, *supra* note 70; GALLIGAN ET AL., *supra* note 70; Hazan, *supra* note 70; Selinger, *supra* note 25.

[73] *See, e.g.*, Sameera Pant et al., *UCLA Decides Not to Implement Facial Recognition Technology After Student Backlash*, DAILY BRUIN (Feb. 19, 2020, 8:03 PM), https://dailybruin.com/2020/02/19/ucla-decides-not-to-implement-facial-recognition-technology-after-student-backlash/; Caroline Haskins, *The New York School District That Used Facial Recognition Now Has to Stop*, BUZZFEED NEWS (Dec. 23, 2020, 4:42 PM), https://www.buzzfeednews.com/article/carolinehaskins1/new-york-stops-school-facial-recognition (last visited Sep 12, 2022); Assemb. B. A6787D 2019–2020 Reg. Sess. (N.Y. 2019); *New York Creates First-in-the-Nation Moratorium on Facial Recognition in Schools*, N.Y. CIV. LIBERTIES UNION (Dec. 22, 2020), https://www.nyclu.org/en/press-releases/new-york-creates-first-nation-moratorium-facial-recognition-schools.

identifying technology" while the state's commissioner of education conducts further studies.[74]

Facial analysis tools, which capture and code facial geometry, are often lumped together under the term "facial recognition."[75] However, different forms of facial analysis differ wildly in their accuracy, degree of intrusion, and scientific foundation.[76]

OPTs' facial analysis features include detecting whether and how many faces are in the testing environment (facial detection), verifying a test-taker's identity (facial verification), and identifying atypical activity (facial characterization and algorithmic behavioral profiling).Vendors use commonplace facial detection and verification technology to authenticate test-takers. Facial verification algorithms compare the resulting "faceprint" to a stored image of the student that is supposed to take an exam—a one-to-one match. Similar systems are commonly used to unlock personal devices.

These facial detection and authentication tools are not as viscerally intrusive as dragnet security surveillance but share many of the same flaws. Facial recognition technologies are much less accurate when applied to people of color, women, or people who are gender nonconforming.[77] As a result, various facial recognition developers and municipalities have also halted development or banned the use of facial recognition technology.[78] While companies and researchers have

---

[74] Assemb. B. A6787D; *New York Creates First-in-the-Nation Moratorium on Facial Recognition in Schools*, *supra* note 73.

[75] *Understanding Facial Detection, Characterization and Recognition Technologies*, FUTURE OF PRIV. F. (Mar. 2018), https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf.

[76] *Id.*

[77] *See, e.g.*, Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 77 (2018) (finding facial recognition less accurate for darker skinned and female faces); Kate Crawford, *Regulate Facial-Recognition Technology*, 572 NATURE 565 (2019); Morgan Klaus Scheuerman et al., *How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services*, 3 PROC. ACM HUMAN-COMPUTER INTERACTION 1 (2019) (finding facial recognition misclassifies the identity of transgender and nonbinary individuals).

[78] Jeffrey Dastin, *Amazon Extends Moratorium on Police Use of Facial Recognition Software*, REUTERS (May 18, 2021, 11:12 AM), https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/; Martin Kaste, *Cities Are Weighing the*

improved facial analysis accuracy across diverse populations,[79] OPTs often use low-cost tools far below state-of-the-art standards.[80] Consequently, proctoring vendors may mistakenly flag certain racial groups more frequently than others.[81]

Proctoring companies could improve their systems to be more accurate across diverse populations. Proctorio took a step to address accuracy problems by hiring a third-party auditor to reduce bias in its facial detection features.[82] However, it is unclear whether this was an empty gesture. Although the company makes information about the bias audit available to customers, it has not publicly disclosed any details.[83] In contrast to security audits featured prominently on Proctorio's website,[84] the vendor buries information about bias audits in a blog post, only noting that auditors "found no measurable (statistically significant) bias" in the company's updated face-detection algorithm. Notably, the company has not indicated any attempt to audit its automated cheating detection systems, which, as the next section discusses, are not only biased but lacking scientific support.

2. Unproven and Biased Algorithmic Profiling

OPTs' facial characterization and behavioral profiling tools are far more problematic than their facial verification and detection ones. These features are premised upon unproven technologies and crude assumptions that lead to an overwhelming number of false positives—

Dangers and Benefits of Facial Recognition, NPR (June 3, 2021, 4:22 PM), https://www.npr.org/2021/06/03/1003020341/cities-are-weighing-the-dangers-and-benefits-of-facial-recognition; *New York Creates First-in-the-Nation Moratorium on Facial Recognition in Schools*, *supra* note 73; Assemb. B. A6787D.

[79] *See, e.g.*, *How the Accuracy of Facial Recognition Technology Has Improved over Time*, INNOVATRICS: TRUST REP. (Mar. 20, 2021), https://trustreport.innovatrics.com/how-the-accuracy-of-face-recognition-technology-has-improved-over-time/; Tajha Chappellet-Lanier, *Facial Recognition Algorithms Are Getting a Lot Better, NIST Study Finds*, FEDSCOOP (Dec. 3, 2018), https://www.fedscoop.com/facial-recognition-algorithms-getting-lot-better-nist-study-finds/.

[80] Burgess et al., *supra* note 69 (finding that proctoring facial recognition software significantly underperforms, noting that faces from various racial groupings are substantially more likely to trigger false positives or false negatives than would be expected from a state-of-the art model).

[81] *Id.* (finding significant variability in verification steps based on race).

[82] Letter from Mike Olsen to Sen. Richard Blumenthal et al., *supra* note 39.

[83] Audits, PROCTORIO, https://proctorio.com/privacy/audits/ (last visited Nov. 14, 2022).

[84] *Id.*

and a greater likelihood that these will disproportionately harm members of marginalized populations.

Vendors first create a profile of "normal" test-taking behaviors,[85] analyzing factors like students' "movement, eye gaze, background noise, and more for any anomalies that could indicate academic dishonesty."[86] The software then compares test-takers' activity to this baseline.[87] OPTs flag students deviating from this "normal" standard as "suspicious," based partly on standards set by the school.[88]

As a result, OPTs label a startling amount of innocent behavior as suspicious, whether the salient difference is due to skin color, a disability, crowded living environments, or an unusual nervous tic.[89] In 2021, for example, ExamSoft categorized nearly a third of test-takers taking the California Bar Exam as suspected cheaters—only to absolve over 90% of them later.[90] ProctorU's algorithms flag commonplace (and

---

[85] *See, e.g.*, *Flexible Solution for Remote, Computer-Based Assessment*, EXAMSOFT (Oct. 18, 2021), https://examsoft.com/benefits/flexibility/ ("Advanced A.I. software detects abnormal student behavior that may signal academic dishonesty"); PROCTORIO, PROCTORIO MISCONCEPTIONS FAQ 4 (2020), https://www.usi.edu/media/oozd23zq/misconceptions-faq.pdf ("Behavior is flagged based on its stark irregularity compared to the behavior found in other exam attempts."); Swauger, *supra* note 25.

[86] *See, e.g.*, *Flexible Solution for Remote, Computer-Based Assessment*, *supra* note 85; PROCTORIO, *supra* note 85; Swauger, *supra* note 25.

[87] *A Test-takers Guide to Online Proctoring*, EXAMITY, https://www.examity.com/a-test-takers-guide-to-online-proctoring/ (last visited Nov. 14, 2022) ("Software captures audio, motion, and systemic changes during the testing session, identifying aberrant or abnormal behaviors."). Proctorio, for example, analyzes information including student speech and environmental sound, gaze detection, mouse clicks, and how long each student took to complete an exam to detect "abnormal behavior" and calculate a "Suspicion Score" for each student. As of September 2020, Proctorio's training materials noted that "[t]he suspicion level will increase or decrease depending on how heavily each Behaviour Setting is weighted and which abnormalities are enabled." Feathers & Rose, *supra* note 33.

[88] *A Test-takers Guide to Online Proctoring*, *supra* note 87*;* Feathers & Rose, *supra* note 33.

[89] *Id.*

[90] Sam Skolnik, *Ninety Percent of Suspected Cheaters Cleared by California Bar*, BLOOMBERG L., (Dec. 30, 2020, 2:05 PM), https://news.bloomberglaw.com/business-and-practice/ninety-percent-of-suspected-cheaters-cleared-by-california-bar.

foreseeable) remote testing scenarios, such as when someone rubs their eyes repeatedly, a dog barks, or a mother speaks to her child.[91]

The overabundance of false flags reflects a fundamental problem with the underlying premise of automated proctoring: that artificial intelligence can detect cheating by analyzing student activity. In other contexts, vendors and researchers also claim that artificial intelligence can infer emotional states, sexual/political orientation, and criminal predilection from people's physical features and activity. However, considerable evidence indicates that these profiling systems are inaccurate due to individual, cultural, and contextual diversity.[92]

Like phrenology and physiognomy before them, these claims of physical profiling reflect and embed problematic cultural assumptions.[93] OPTs' automated cheating detection tools make similarly speculative inferences based on test-takers' physical and digital activity.[94]

Vendors' algorithmic profiling also relies on several dubious assumptions: that a profile of "normal" test taker behavior exists, that a computer can capture it, and that atypical activity indicates suspicious behavior.[95] However, there is no such thing as "normal" when it comes

---

[91] *ProctorU to Discontinue Exam Integrity Services That Rely Exclusively on AI*, PROCTORU (May 24, 2021, 8:00 AM), https://www.proctoru.com/industry-news-and-notes/proctoru-to-discontinue-exam-integrity-services-that-rely-exclusively-on-ai; *see also Examity Flag Breakdown*, UNIV. OF N.C. AT PEMBROKE, https://www.uncp.edu/sites/default/files/2021-09/Examity%20Flag%20Breakdown.pdf (last visited Nov. 14, 2022) (explaining that Examity's system flags bathroom breaks, reading questions aloud, or children present in a testing space as potential violations).

[92] For example, facial movements are not consistent indicators of individuals' emotional state. *See, e.g.*, Barrett et al., *supra* note 69; Luke Stark & Jevan Hutson, *Physiognomic Artificial Intelligence*, 32 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 922 (2021); Crawford, *supra* note 77; Ifeoma Ajunwa, *Automated Video Interviewing as the New Phrenology*, 36 BERKELEY TECH. L.J. (2022).

[93] *See* Barrett et al., *supra* note 69; Stark & Hutson, *supra* note 92; Crawford, *supra* note 77; Ajunwa, *supra* note 92.

[94] *See, e.g.*, Data Analytics, *Track Integrity for Test Taker Success*, PROCTORIO https://proctorio.com/platform/data-analytics (last visited Feb. 24, 2021) [https://perma.cc/W6MN-QNHC] ("Aggregate data can spot general trends such as rates of testing violations, while individualized data can track test-takers over the length of their academic careers and even assign suspicion ratings"). *See generally* Ben Williamson, *Coding the Biodigital Child: The Biopolitics and Pedagogic Strategies of Educational Data Science*, 24 PEDAGOGY, CULTURE & SOC'Y 401 (2016).

[95] *See* Zoe Guy, *Activist Lydia X. Z. Brown on Disability Justice, Mutual Aid, and How Race and Disability Intersect*, MARIE CLAIRE (Mar. 18, 2021),

to students and their environments—or, for that matter, humanity in general.[96] These crude presumptions disproportionately harm already marginalized students, especially those with disabilities.[97]

Take, for example, being left-handed. Because being right-handed is more common, algorithms could learn to associate picking up a glass or writing with the right hand as "normal." Left-handed movement would be atypical. Under this logic, OPT cheating detection tools might flag left-handed students for suspicious behavior. Hopefully, being left-handed does not lead to more OPT flags—it is not exceedingly rare, and perhaps vendors have taken such an obvious characteristic into account. But students and teachers have no way of knowing if this common behavior will be flagged.

Overly aggressive cheating detection undermines students' academic performance. Too many false flags may lock students out of an exam. In the worst cases, they could lead teachers to charge innocent students with cheating. These problems harm students even if a further investigation finds no wrongdoing. Cheating allegations can damage students' reputations with professors and peers, decimating their academic careers and job prospects. News of accusations may surface online, creating a damning digital footprint. Instructors may also distrust students with high suspicion scores even in the absence of a technical lockout or formal cheating allegations.

OPTs try to compensate for flawed software by requiring students to comply with impossible physical constraints.[98] Vendors prohibit students from standing up, moving out of view, or looking

---

https://www.marieclaire.com/politics/a35866693/lydia-x-z-brown-interview-2021/; 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/; Asher-Schapiro, *supra* note 24.

[96] Guy, *supra* note 95; Brown, *supra* note 95; Asher-Schapiro, *supra* note 24; INT'L PRIVACY SUBCOMM. OF THE ATP SECURITY COMM., *supra* note 45, at 2; Alex Engler, *For Some Employment Algorithms, Disability Discrimination by Default*, BROOKINGS (Oct. 31, 2019), https://www.brookings.edu/blog/techtank/2019/10/31/for-some-employment-algorithms-disability-discrimination-by-default/.

[97] Guy, *supra* note 95; Brown, *supra* note 95; Asher-Schapiro, *supra* note 24; INT'L PRIVACY SUBCOMM. OF THE ATP SECURITY COMM., *supra* note 45; Engler, *supra* note 96.

[98] Patil & Bromwich, *supra* note 24; Chin, *supra* note 25.

away from the screen.[99] Their systems interpret a student talking aloud and "excessive movement" as suspect.[100] As a result, students divert considerable attention to monitoring their behavior and physical environment.[101] Unsurprisingly, stressed students may not perform as well.[102] As in traditional test settings,[103] anxiety reduces performance during remote testing, particularly in online proctoring conditions.[104]

3. Intrusive Biometric Surveillance

Vendors and schools defend online proctoring as simply a remote version of traditional in-person proctors. However, OPT "monitoring" is not just a digital analog of in-person proctors observing a school room full of students. OPTs subject students to considerably more surveillance than in-person proctoring—peering into and

---

[99] *See, e.g.*, *A.I. Proctoring: Invigilation Exam Day Guide*, *supra* note 46; Jenny Rankin, *What Am I Allowed and Not Allowed to Do During My Exam?*, PROCTORU (Nov. 1, 2023 9:20 PM), https://support.proctoru.com/hc/en-us/articles/360043127892-What-am-I-allowed-and-not-allowed-to-do-during-my-exam-.

[100] *See, e.g.*, *A.I. Proctoring: Invigilation Exam Day Guide*, *supra* note 46; Rankin, *supra* note 99.

[101] Raman et al., *supra* note 3; Selwyn et al., *supra* note 3; Daniel Woldeab & Thomas Brothen, *Video Surveillance of Online Exam Proctoring: Exam Anxiety and Student Performance*, 36 INT'L J. E-LEARNING & DISTANCE EDUC. 1 (2021); Patil & Bromwich, *supra* note 24; Coghlan et al., *supra* note 12; 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/; Daniel Woldeab & Thomas Brothen, *21st Century Assessment: Online Proctoring, Test Anxiety, and Student Performance*, 34 INT'L J. E-LEARNING & DISTANCE EDUC. 1 (2019); Daniel Woldeab et al., *Under the Watchful Eye of Online Proctoring*, *in* INNOVATIVE LEARNING & TEACHING: EXPERIMENTS ACROSS THE DISCIPLINES 147 (Ilene D. Alexander & Robert K. Poch eds., 2017); Natasha Singer, *Online Test-Takers Feel Anti-Cheating Software's Uneasy Glare*, N.Y. TIMES (Apr. 5, 2015), http://www.nytimes.com/2015/04/06/technology/online-test-takers-feel-anti-cheating-softwares-uneasy-glare.html.

[102] Rianne Conijn et al., *The Fear of Big Brother: The Potential Negative Side-effects of Proctored Exams*, 38 J. COMPUT. ASSISTED LEARNING 1521 (2022); Sandra Gudiño Paredes et al., *Remote Proctored Exams: Integrity Assurance in Online Education?*, 42 DISTANCE EDUC. 200 (2021); Prakash Sinha & Aman Yadav, *Remote Proctored Theory and Objective Online Examination*, 11 INT'L J. ADVANCED NETWORKING & APPLICATIONS 4494 (2020).

[103] *See, e.g.*, C. Cassady & Ronald E. Johnson, *Cognitive Test Anxiety and Academic Performance*, 27 CONTEMP. EDUC. PSYCH. 270 (2002).

[104] Woldeab & Brothen, *supra* note 101.

collecting data about students' bodies, movements, and intimate spaces.[105]

Instead of the breadth of surveillance imposed by campus security systems, OPTs mine data for depth, analyzing the smallest details of students' digital activity, physical behavior, and testing environment.[106] Artificial intelligence then extracts far more information from this data than any human could perceive—analyzing eye movements, shadows, reflections, and more.[107] The in-person equivalent of OPT surveillance would be a human supervisor sitting near a test-taker and staring at the test-taker constantly throughout the exam, using advanced technology to observe, record, and dissect every micromovement.[108]

Online proctoring systems collect a greater quantity, breadth, and detail of information than is possible with human proctors.[109] Examity, for instance, collects biometric data from students that may include "fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting."[110] Biometric monitoring of students—including children—raises concerns beyond the potential to penalize marginalized and nonconforming students, as described above.[111] For example, it includes immutable identifying

---

[105] Coghlan et al., *supra* note 12, at 1952; Sarah Khan & Rashid Azim Khan, *Online Assessments: Exploring Perspectives of University Students*, 24 EDUC. & INFO. TECHS. 661 (2019); Bill Fitzgerald, *There Is No Such Thing as an "Online Proctoring System,"* FUNNY MONKEY (Aug. 21, 2021), https://www.funnymonkey.com/2021/08/there-is-no-such-thing-as-an-online-proctoring-system/; Selinger, *supra* note 25.

[106] *A.I. Proctoring: Invigilation Exam Day Guide*, *supra* note 46 (analyzing "movement, eye gaze, background noise, and more"); PROCTORU, https://www.proctoru.com/harnessing-the-power-of-artificial-intelligence7/24/2021 (last visited July 24, 2021) (analyzing "shadows, whispers or low sound levels, reflections, etc., that may otherwise go unnoticed").

[107] *A.I. Proctoring: Invigilation Exam Day Guide*, *supra* note 46; PROCTORU, *supra* note 106.

[108] Coghlan et al., *supra* note 12, at 1596.

[109] *Id.*; Khan & Khan, *supra* note 105; Fitzgerald, *supra* note 105; Selinger, *supra* note 25.

[110] *Product & Services Privacy Policy*, EXAMITY, https://on.examity.com/V5/privacy.

[111] *Stop Spying on Kids*, FIGHT FOR THE FUTURE, https://www.stopspyingonkids.com/ (last visited Nov. 16, 2022); *End Child Surveillance*, FIGHT FOR THE FUTURE, https://www.endchildsurveillance.com (last visited Nov. 16, 2022); U.K. DEP'T OF EDUC., PROTECTION OF BIOMETRIC INFORMATION OF CHILDREN IN SCHOOLS AND COLLEGES 13 (2021); Lindsey Barrett, *Ban Facial Recognition Technologies for Children—And for Everyone Else*, 26 B.U. J. SCI. & TECH. L. 223 (2020); Nila Bala, *The Danger of Facial Recognition in Our Children's Classrooms*, 18 DUKE L. & TECH. REV. 249 (2020).

details that students cannot change in the event of a security breach or unauthorized access.

Remote human proctors use videoconferencing to closely observe individuals or small groups of students in their personal spaces, rather than a roomful of test-takers on school premises.[112] Proctoring technologies also capture audiovisual data from students' environments with web cameras and microphones to detect prohibited materials or the presence of people whom students might ask for help.[113] Respondus's system, for example, requires students to capture 360-degree scans of their surroundings.[114]

OPTs also use computer logging systems and web cameras to surveil students and their surroundings.[115] Some scan personal data on students' devices to look for copied questions.[116] Their digital monitoring tools take what researchers have called a "kitchen sink" approach, accessing personal files and capturing keystrokes, screenshots, and audiovisual feeds.[117] These features are not just atypical—they would be considered malware outside of the online proctoring context.[118]

This invasive OPT surveillance is detrimental to students' success and emotional well-being. Surveillance in high-stakes situations lowers students' academic performance,[119] disproportionately harming marginalized students.[120] Live remote monitoring, for example, lowered the scores of students already anxious about testing.[121] Camera

---

[112] Coghlan et al., *supra* note 12; Chin, *supra* note 25 (noting that a former Examity proctor said, "[W]e closely watch the face of the student to see if there is something suspicious, like suspicious eye movements, or if the student is trying to mumble something to somebody else outside the room").

[113] Arnò et al., *supra* note 47.

[114] *See, e.g.*, *Room and Desk Scan Instructions*, VERIFICIENT SUPPORT (Nov. 9, 2022, 9:00 PM), https://verificient.freshdesk.com/support/solutions/articles/1000287710-room-and-desk-scan-instructions.

[115] Burgess et al., *supra* note 69.

[116] Ben Blum-Smith, *Remote Proctoring: A Failed Experiment in Control*, AM. MATHEMATICAL SOC'Y: BLOGS (Jan. 19, 2021), https://blogs.ams.org/matheducation/2021/01/19/remote-proctoring-failed-experiment-in-control/.

[117] Burgess et al., *supra* note 69.

[118] *Id.*

[119] Elana Zeide, *The Credentialing Effect: Psychological Effects of Ubiquitous Capture and Constant Evaluation*, Privacy Law Scholars Conference (Jun. 2016) (draft on file with author); *see, e.g.*, Jeffrey R. Stowell & Dan Bennett, *Effects of Online Testing on Student Exam Performance and Test Anxiety*, 42 J. EDUC. COMPUTING RSCH. 161 (2010).

[120] Zeide, *supra* note 119; Conijn et al., *supra* note 102.

[121] Woldeab & Brothen, *supra* note 101, at 1 ("This study shows that high trait test anxiety results in lower exam scores and that this is especially true for those students with high text anxiety taking exams in an online proctored setting.").

surveillance also exacerbates anxiety, particularly for marginalized students.[122]

Intrusive monitoring in educational spaces leads to problematic pedagogical consequences as well.[123] Neil Richards has noted that "intellectual privacy" is essential to free expression and human development.[124] Even the threat of surveillance discourages participation and subconsciously prompts students to censor what they perceive as unpopular views.[125] Just as significantly, OPTs normalize surveillance for an entire generation.[126]

4. Placebo Proctoring

Despite their extensive surveillance and "cutting edge" artificial intelligence, proctoring technologies may not even detect academic misconduct.[127] A recent study, for example, found that Proctorio did not catch test-takers who purposefully cheated as part of an experiment.[128] Studies claiming that OPTs deter cheating often do so based on

---

[122] Conijn et al., *supra* note 102 (noting that proctoring did not change students' temptation to cheat or performance but led to higher levels of anxiety, especially for students concerned about access to reliable technology and gender); Gudiño Paredes et al., *supra* note 102; Kristie Kaczmarek et al., *Eye in the Sky: Student Perceptions of Secure Remote Examinations*, 85 J. DENTAL EDUC. 1949 (2021).

[123] *See* Elana Zeide, *The Structural Consequences of Big Data-Driven Education*, 5 BIG DATA 164 (2017); Zeide, *supra* note 119; Conijn et al., *supra* note 102.

[124] NEIL M. RICHARDS, INTELLECTUAL PRIVACY 165 (2015).

[125] *Id.*; Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 490–92, 501–06 (2015).

[126] 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/; Selinger, *supra* note 25.

[127] Laura Bergmans et al., *On the Efficacy of Online Proctoring Using Proctorio*, *in* 2 PROCEEDINGS OF THE 13TH INTERNATIONAL CONFERENCE ON COMPUTER SUPPORTED EDUCATION 279 (Beno Csapó & James Uhomoibhi eds., 2021); *see also Report of the Academic Integrity Committee About Online Testing and Assessment*, UNIV. OF TEX. AT AUSTIN (Aug. 2021), https://utexas.app.box.com/s/vpy39q600ffgogmc3rc3fqzxhdva5qgo (noting that extensive use of proctoring tools during 2020–21 led to only twenty-seven cases referred to the Student Conduct and Academic Integrity office as potential violations of academic integrity, of which only thirteen were upheld).

[128] Bergmans et al., *supra* note 127.

questionable metrics.[129] Many find that students score lower in online proctoring conditions and conclude this reflects thwarted misconduct.[130] However, poor performance could just as easily reflect other aspects of remotely proctored exams, including technical difficulties and increased anxiety.[131]

To the degree that proctoring technologies do prevent cheating, research suggests that deterrence is not due to "cutting-edge" AI technologies but the mere presence of a proctoring system.[132] One study found that "[o]nline proctoring is . . . best compared to taking a placebo: it has some positive influence, not because it works but because people believe that it works, or that it might work."[133] In sum, insufficient evidence supports vendors' claims.

C. Sociotechnical Shortcomings

It is important to consider education technology not in isolation but as part of a sociotechnical system, and to identify which issues stem from vendors' technology, schools' implementation, or instructors' pedagogical choices. A systemic perspective is particularly crucial with decision support tools like OPTs, where schools choose which features to use, what settings to apply, and when educators should double-check automated assessments.

---

[129] *See, e.g.*, Gemma Cherry et al., *Do Outcomes from High Stakes Examinations Taken in Test Centres and via Live Remote Proctoring Differ?,* 2 COMPUTS. & EDUC. OPEN 100061 (2021); Patricia A. Goedl & Ganesh B. Malla, *A Study of Grade Equivalency Between Proctored and Unproctored Exams in Distance Education*, 34 AM. J. DISTANCE EDUC. 280 (2020); Diane J. Prince et al., *Comparisons of Proctored versus Non-Proctored Testing Strategies in Graduate Distance Education Curriculum*, 6 J. COLL. TEACHING & LEARNING 51 (2009); Helaine Mary Alessio et al., *Examining the Effect of Proctoring on Online Test Scores*, 21 ONLINE LEARNING 146 (2017).

[130] Cherry et al., *supra* note 129; Goedl & Malla, *supra* note 129; Prince et al., *supra* note 129; Alessio et al., *supra* note 129.

[131] Raman et al., *supra* note 3; Selwyn et al., *supra* note 3; Woldeab & Brothen, *supra* note 101; Patil & Bromwich, *supra* note 24; Coghlan et al., *supra* note 12; Jung, *supra* note 101; Woldeab & Brothen, *supra* note 101; Woldeab et al., *supra* note 101; Singer, *supra* note 101.

[132] Bergmans et al., *supra* note 127; *see also Report of the Academic Integrity Committee About Online Testing and Assessment*, *supra* note 127; Jacob Pleasants et al., *Cheating on Unproctored Online Exams: Prevalence, Mitigation Measures, and Effects on Exam Performance*, 26 ONLINE LEARNING 268 (2022) ("However, when students received a warning that we had technology that could detect cheating, coupled with threats of harsh penalties, cheating behavior dropped to 15% of students.").

[133] Bergmans et al., *supra* note 127 ("The most important findings were that none of the cheating students were flagged by Proctorio . . . .").

1. The "Decision-Support" Excuse

Vendors deflect criticism for inaccuracies by characterizing their services as decision support—schools, not their software, make the ultimate determination about students' misconduct.[134] An ExamSoft blog post, for example, is titled: "Clearing up Confusion: Flagging Isn't the Same as Cheating."[135] As the pandemic progressed and evidence indicated a lack of institutional oversight, it became irresponsible, if not disingenuous, for vendors to market their services as mere "decision support." ProctorU acknowledged as much and stopped offering AI-only proctoring services in May 2021.[136] The company's founder noted that automated proctoring systems often flag students for innocent behavior and unfairly implicate test-takers absent human review.[137] Given automated proctoring's high error rates, vendors' "decision support" model essentially asks educators to perform quality control on companies' behalf—an impossible task.

Vendors offering automated cheating detection want it both ways: to claim that their systems can accurately identify misconduct but bear no responsibility for frequent inaccuracies. This would be less egregious if the artificial intelligence used in proctoring technologies was sufficiently accurate to flag only a few suspicious events across an entire class, making it plausible that educators could check for automation errors. But when 90% of flags might be false, as they were when ExamSoft protected the California Bar Exam, it is impossible to expect teachers to double-check automated flags.

2. Institutional Lack of Oversight and Due Process

Schools' implementation of proctoring technologies rarely addressed OPTs' inaccuracy, bias, or intrusive surveillance. An

---

[134] *See, e.g.*, *id.*; *see also* Letter from Sabastian Vos to Sen. Richard Blumenthal et al., *supra* note 39.
[135] John-Paul Gaconnier, *Clearing Up Confusion: Flagging Isn't Cheating*, EXAMSOFT (Jan. 6, 2021), https://examsoft.com/resources/flagging-isnt-cheating.
[136] The company now uses trained human proctors for every test session. *ProctorU to Discontinue Exam Integrity Services That Rely Exclusively on AI*, *supra* note 91.
[137] *Id.*

abundance of anecdotal evidence suggests that schools adopted proctoring technologies hastily and deployed them haphazardly.[138]

Some gave teachers little more than directions for how students should register and sign into the systems.[139] Many schools also did not provide students or teachers context for OPTs or information about what steps either group should take if they felt disadvantaged by technical glitches or unfairly flagged for innocent behavior but rather merely linked to companies' resources and literature.[140] Institutional reference and support pages often simply linked to companies' resources.[141]

Instructors received minimal information about how to interpret proctoring reports, what scores were sufficient to support an allegation of cheating, and what patterns might indicate software error rather than student misconduct.[142] One teacher, for example, chastised students for moving their heads and eyes a certain number of times within a few minutes, insinuating that this statistic revealed students were cheating.[143] But the mere frequency of students' movements doesn't reliably indicate academic impropriety.

Untrained and overwhelmed teachers often took the accuracy of automated systems at face value.[144] Only 11% of ProctorU's test

---

[138] *See, e.g.*, Lindsay McKensie, *Time to Rethink AI Proctoring: Are Colleges Checking AI's Work in Remote Exam Proctoring?*, INSIDE HIGHER ED (May 28, 2021), https://www.insidehighered.com/news/2021/05/28/are-colleges-checking-ais-work-remote-exam-proctoring; Barrett, *supra* note 25; Benjamin Herold, *The Scramble to Move America's Schools Online*, EDUC. WK. (Mar. 27, 2020), https://www.edweek.org/technology/the-scramble-to-move-americas-schools-online/2020/03 (reviewing the rushed nature of the decision to move schools online as a survival technique without the opportunity to equip students fully, train teachers adequately, or consider the long-term impacts of online learning).

[139] Mussachio, *supra* note 33.

[140] Charles Logan, *Toward Abolishing Online Proctoring: Counter-Narratives, Deep Change, and Pedagogies of Educational Dignity*, 20 J. INTERACTIVE TECH. & PEDAGOGY 19 (2021).

[141] Kimmons & Velestsianos, *supra* note 4.

[142] @LegendAriee, X (Sept. 10, 2020, 12:45 PM), https://twitter.com/LegendAriee16/status/1304098649186742273.

[143] The teacher noted that students had resized their browsers, which she interpreted as the students viewing prohibited websites. *Id.* She noted that one student had "776 head and eye movements" in a six-minute time span, while another had 624 similar movements within eight minutes, stating that "this is an indication of eyes moving away from the screen," insinuating that doing so indicated impropriety. *Id.* (emphasis omitted). She concluded with the warning "I would hate to have to write you up for online cheating which gets filed in the Dean's office." *Id.* (emphasis omitted).

[144] McKensie, *supra* note 138; Scott Jaschik, *ProctorU Abandons Business Based Solely on AI*, INSIDE HIGHER ED (May 23, 2021), https://www.insidehighered.com/news/2021/05/24/proctoru-abandons-business-based-solely-ai; Kelley, *supra* note 23.

administrators reviewed exam sessions tagged by their AI for suspicious activity.[145] The University of Iowa similarly reviewed only 14% of test sessions flagged for possible rule violations.[146]

Teachers' failure to scrutinize OPT reports may reflect unconscious automation bias.[147] But in most cases, educators simply didn't have the time to review OPT reports, especially given the high volume of activity flagged as suspicious.[148] ProctorU estimated that it would take teachers nine hours to review a short exam given to 150 students.[149] It is unrealistic and untenable for schools to expect already overwhelmed instructors to take this time to correct proctoring software's mistakes.[150] Further, few schools have established formal procedures for test-takers to challenge OPT reports.[151]

Untrained educators also could not communicate the benefits and limitations of online proctoring to students and parents—or what measures were in place to account for technological errors. The resulting absence of transparency, communication, and oversight stoked test-takers' anxieties.[152] Students did not know what behavior would be problematic, when flags would lead to cheating allegations, and what to do when the software didn't work as expected.[153] They did not know whether technical errors would lead to unfair accusations, discipline, or marred academic records absent clear oversight protocols and appeal processes. In this vacuum, students understandably attempted to guess and control for behavior that OPTs might flag—some going so far as to urinate in their seats rather than take bathroom breaks.[154]

Given these problems, the current proctoring sociotechnical system is unacceptably flawed—inaccurate, inequitable, invasive, and

---

[145] *See* Jaschik, *supra* note 144.
[146] *Id.*
[147] Kate Goddard et al., *Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators*, 19 J. AM. MED. INFORMATICS ASS'N. 121 (2012).
[148] *See, e.g.*, MacFarland, *supra* note 40 ("[E]ven human beings aren't always very good at discerning between normal activities and cheating on a video tape. It takes training and time – which academics don't have."); *ProctorU to Discontinue Exam Integrity Services That Rely Exclusively on AI*, *supra* note 91.
[149] *See, e.g.*, MacFarland, *supra* note 40.
[150] *See supra* Section I.C.B (noting schools' failure to review automated reports in many cases).
[151] Kelley, *supra* note 23.
[152] *See, e.g.*, Patil & Bromwich, *supra* note 24; Chin, *supra* note 25.
[153] *See supra* Section I.A–.B.
[154] *Cheating-Detection Companies*, *supra* note 24.

ineffective. Between vendors' unproven technologies and schools' haphazard implementation, online proctoring risks unfairly punishing innocent students. The next section explores avenues that students might take to obtain due process and promote reform. The law already has tools to address some of these problems but not particularly well.

II. WEAK LEGAL PROTECTION AND FERPA'S STOPGAP SOLUTION

Students or advocates might pursue strategies across several legal regimes to respond to and prompt reform of proctoring technologies, including biometric and student privacy, consumer protection, and antidiscrimination law.[155] However, these avenues are both uncertain and insufficient.

Student privacy laws focus on preventing unauthorized disclosure or commercialization of student information, not protecting them against problematic school-approved technologies or surveillance.[156] However, students can use FERPA to access—and possibly amend, contest, and annotate—OPTs' algorithmic inferences. Students in Illinois may be able to recover compensation against OPTs under the state's biometric privacy statute (BIPA).[157] However, BIPA liability will likely lead to token disclosure rather than fundamental reform; a few states have student biometric privacy prohibitions but ignore them.

With sufficient supporting evidence, the FTC could find proctoring technology vendors' overblown and unproven claims to constitute deceptive trade practices.[158] More tenuously, the agency could use pandemic proctoring as an opportunity to regulate artificial intelligence more aggressively by finding vendors' use of AI unfair.[159] However, while many OPT practices don't meet emerging civil society and industry standards for the ethical use of artificial intelligence,[160] these nascent and often vague guidelines are unlikely to meet the agency's criteria for established public policy.
Finally, antidiscrimination claims face significant substantive and procedural obstacles.[161]

---

[155] There may also be viable Fourth Amendment claims in unusual circumstances, as was the case in Ogletree v. Cleveland State Univ., No. 21-cv-00500, 2022 WL 17826730 (N.D. Ohio Dec. 20, 2022). *See supra* note 7.
[156] *See infra* Section II.A.
[157] 740 ILL. COMP. STAT. ANN. 14/15 (2022); *see infra* Section II.B.
[158] *See infra* Section II.C.1.
[159] *See infra* Section II.C.2.
[160] *See infra* Section II.C.2.
[161] *See infra* Section III.D.

A. FERPA's Leverage and Limitations

Student privacy law seems like a natural place for aggrieved students and advocates to turn.[162] However, student privacy law does not directly address the harms caused by schools' use of education technologies for assessments.[163] This article introduces a new strategy that leverages students' rights under FERPA to promote transparency and due process without waiting on uncertain enforcement.

FERPA, the most prominent federal student privacy law, limits how schools can disclose, use, and maintain personally identifiable student information as a condition of federal funding.[164] It gives parents and eligible students[165] two fundamental rights: the right to consent before school disclosure of personally identifiable student information and to access and challenge information in their education records.[166]

---

[162] Bar exam test takers are not covered by FERPA, which applies only to educational agencies and institutions that receive federal funding. 20 U.S.C. § 1232g. They are also not covered by states' education data privacy laws, which typically apply to publicly funded K-12 schools. *See, e.g.*, FLA. STAT. § 1002.22(1)(a) (2023).

[163] 20 U.S.C. § 1232g; 34 C.F.R. § 99 (2022); Gonzaga Univ. v. Doe, 536 U.S. 273 (2002) (holding that FERPA does not give rise to a private right of action); Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339 (2016) (explaining that FERPA governs schools' disclosure, not their use of personally identifiable student information).

[164] FERPA requires educational institutions and agencies ("schools") to follow its dictates as a condition of receiving federal funding. *See* 20 U.S.C. §§ 1232g(a)(1)(A)–(B), 1232g(b)(1)–(2) (stating that funds shall not be made available under any applicable program to educational agencies or institutions that have a policy or practice of denying or effectively preventing the exercise of rights assured under FERPA or of permitting the release of educational records without written consent). Primary and secondary public schools, and most public and private postsecondary institutions, fall under its purview.

[165] When a student turns eighteen years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). 20 U.S.C. § 1232g(d); 34 C.F.R. §§ 99.3, 99.5. When referring to FERPA rights, I use the term "students" or "parents" for the sake of brevity to include both parents and eligible students.

[166] 20 U.S.C. § 1232g(b)(1) (establishing the right to consent); 20 U.S.C. § 1232g(a)(1)(A) (establishing the right to inspect and review).

1. FERPA's Inadequate Right of Consent

FERPA's right of consent seeks to protect against unauthorized disclosure and noneducational use of personally identifiable student information.[167] Schools must get parents' or eligible[168] students' consent before disclosing personally identifiable student information.[169] However, the law's exceptions now overshadow the rule.[170] Schools may share covered student information without consent under the school official exception, as long as the recipient furthers a "legitimate educational interest" and schools retain "direct control" over the use and maintenance of students' data.[171]

The standard for legitimate educational interests is notoriously low; most school policies use a circular definition covering any school-authorized use.[172] Schools' use of technology to prevent cheating and facilitate remote assessment during the pandemic easily passes that bar. The criteria for "direct control" remain amorphous, but often turn on whether vendors have too much discretion to use covered information for unauthorized purposes.[173] The more sophisticated OPTs have terms

---

[167] 20 U.S.C. § 1232g(d); 34 C.F.R. §§ 99.3, 99.5.
[168] 20 U.S.C. § 1232g(b)(1) (establishing the right of consent).
[169] Zeide, *supra* note 163.
[170] *Id.*
[171] 34 C.F.R. § 99.31(a)(1)(i)(A) (establishing the school-official exception requirement that "disclosure is to other school officials, including teachers, within the agency or institution whom the agency or institution has determined to have legitimate educational interests."); 34 C.F.R. § 99.31(a)(1)(i)(B)(2) (establishing the school-official exception requirement that the disclosed information be "under the direct control of the agency or institution with respect to the use and maintenance of education records"). The recipient must also be providing a service or function for which the school would otherwise use staff. 34 C.F.R. § 99.31(a)(1)(i)(B).
[172] A "legitimate educational interest" has been interpreted by ED as "the need to perform an official task that requires access" to personally identifiable student information in student records. *See* Letter from LeRoy S. Rooker, Director, U.S. Dep't of Educ., Fam. Pol'y Compliance Off., to John R. Leitzel, President, Univ. of New Hampshire 3, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/unh.pdf; Elana Zeide, *The Limits of Education Purpose Limitations*, 71 U. MIAMI L. REV. 493 (2017).
[173] U.S. DEP'T OF EDUC., PRIVACY TECH. ASSISTANCE CTR., PROTECTING STUDENT PRIVACY WHILE USING ONLINE EDUCATIONAL SERVICES: REQUIREMENTS AND BEST PRACTICES 9 (2014), https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf; Family Education Rights and Privacy, 73 Fed. Reg. 74806, 74816 (Dec. 9, 2008) (to be codified at 34 C.F.R. pt. 99) ("[Direct control] includes ensuring that outside parties that provide institutional services or functions as 'school officials' . . . do not maintain, use, or redisclose education records except as directed by the agency or institution that disclosed the information.").

of service that satisfy the requirement by, for example, limiting their ability to redisclose identifiable student data and agreeing to delete it upon schools' requests.[174]

FERPA also doesn't help students when teachers violate its requirements by sharing personal student information for non-educational purposes.[175] The statute aims to ensure general compliance, not compensate students for harm.[176] To do so, it conditions federal funding on schools' overall compliance with the statute's requirements.[177] FERPA does not impose direct consequences for occasional violations. Instead, schools must engage in a "policy or practice" of noncompliance before ED proceeds to enforcement.[178] Even then, ED's Student Privacy Policy Office will attempt to bring schools into compliance before proceeding to withdraw federal funds.[179] In fact, the agency has never imposed this "nuclear option."[180] As a result, FERPA imposes negligible direct consequences unless schools repeatedly and purposefully violate its requirements.[181]

---

[174] *See, e.g.*, *Privacy and Security*, EXAMITY, https://www.examity.com/features/privacy-and-security/ (last visited Nov. 17, 2022) ("We do not sell, share, or market your data to third-parties" and "We do not store your data past the length of our contract with your institution/organization.").

[175] Gonzaga Univ. v. Doe, 536 U.S. 273 (2002). *See* Elana Zeide, *supra* note 163; Stephanie D. Humphries, *Institutes of Higher Education, Safety Swords, and Privacy Shields: Reconciling FERPA and the Common Law*, 35 J. COLL. & U. L. 145, 160–64 (2008). In several instances, OPS executives shared students' personally identifiable information in ways that violated FERPA's mandates. ProctorU's CEO created a "Hall of [Cheating] Fame" video, and Proctorio's CEO shared information about a student criticizing his product in an online chat. *Mass School Closures*, *supra* note 24; Namman Zhou, *CEO of Exam Monitoring Software Proctorio Apologises for Posting Student's Chat Logs on Reddit*, GUARDIAN (July 1, 2020, 2:27 AM), http://www.theguardian.com/australia-news/2020/jul/01/ceo-of-exam-monitoring-software-proctorio-apologises-for-posting-students-chat-logs-on-reddit. These clearly do not serve legitimate educational interests as required under the school official exception. But FERPA applies to federally funded schools (and education agencies)—not vendors. Zeide, *supra* note 163. At best, ED could punish a vendor indirectly by prohibiting a school from sharing information with the vendor for at least five years. 34 C.F.R. § 99.67 (2022). However, the Department has never exercised this authority.

[176] *Gonzaga*, 536 U.S. 273.

[177] 20 U.S.C. § 1232g(b)(1).

[178] 34 C.F.R. §§ 81.3, 99.67.

[179] *Id.*

[180] Zeide, *supra* note 163.

[181] *Id.*

2. FERPA's Overlooked Rights of Inspection and Review

Students can wield FERPA's often-overlooked second set of rights to obtain transparency and promote due process even in the absence of agency enforcement. The statute's right "to inspect and review" students' education records ensures "that educational records do not contain inaccurate, misleading, or inappropriate information."[182] Education records include the data that vendors maintain on a school's behalf.[183]

FERPA's regulations clarify that schools must respond to reasonable requests to explain and interpret the records.[184] This right to an explanation extends beyond students' personally identifiable information if more information is necessary to understand and interpret the information in education records.[185] For example,

---

[182] 20 U.S.C. § 1232g(a)(1) (granting parents "the right to inspect and review the education records of their children"); 34 C.F.R. § 99.10.

[183] 20 U.S.C. § 1232(g); 34 C.F.R. § 99.3 ("Education records is defined as information that is directly related to a student and maintained by an educational agency or institution, or by a party acting for the agency or institution."); Letter from LeRoy S. Rooker, Director, U.S. Dep't of Educ., Fam. Pol'y Compliance Off., to Gary S. Matthews, Superintendent, Carroll Indep. Sch. Dist. 3 (Sept. 13, 2005) [hereinafter The Carroll Letter], https://studentprivacy.ed.gov/sites/default/files/resource_document/file/carrollisd091305.pdf ("[U]nder FERPA, the District must allow a parent to inspect and review personally identifiable test protocols and other records maintained by professionals . . . for the District").

[184] 34 C.F.R. § 99.10(c) (establishing that schools must "respond to reasonable requests for explanations and interpretations of [education] records"); 34 C.F.R. § 300.562(b)(1); *Does a School Have to Explain or Interpret Education Records When Requested by a Parent or Eligible Student?*, U.S. DEP'T OF EDUC., https://studentprivacy.ed.gov/faq/does-school-have-explain-or-interpret-education-records-when-requested-parent-or-eligible (last visited Nov. 17, 2022); The Carroll Letter, *supra* note 183.

[185] The Carroll Letter, *supra* note 183, at 3 ("For your information, parents do not have a right under FERPA to inspect and review records that are not directly related or personally identifiable to a student. For example, a test protocol or question booklet that is separate from the sheet on which a student records answers and that is not personally identifiable to the student is not considered the student's 'education record' under FERPA. However, both FERPA and Part B provide that an educational agency or institution (under FERPA) and a participating agency (under Part B) must respond to reasonable requests for explanations and interpretations of education records. 34 C.F.R. § 99.10(c); 34 C.F.R. § 300.562(b)(1). Accordingly, if an educational agency or institution or participating agency maintains a copy of a student's test answer sheet, then it must provide the parent with an explanation and interpretation of the record, which could involve showing the parent the test question booklet, reading the questions

FERPA's right of access includes the right to review students' answers to a test as personally identifiable information maintained in a student's education record.[186] However, the answer key to the test might not contain any personal information related to any student.[187] Nevertheless, a student would need to see at least an answer key in order to assess whether the answers in their education record are accurate.[188] As a result, a school might have to share more non-personal information, like the questions on the test and grading criteria, to explain the information.[189]

Students could leverage FERPA's right of access as follows. Students would request access to their proctoring-related records, which contain personally identifiable information.[190] Students would also request access to the underlying data and algorithmic model that misidentified, flagged, and scored their activity. Assuming that schools do not have this data on hand, they would relay this request to the vendor and provide it to students within forty-five days.[191]

Schools and vendors may balk at providing this access; it is difficult and often expensive to create tools that permit students to view their data without compromising other students' privacy or revealing

---

to the parent, or providing an interpretation for the responses in some other manner adequate to inform the parent."); *see also* Letter from LeRoy S. Rooker, Director, U.S. Dep't of Educ., Fam. Pol'y Compliance Off., to Moriah Central Sch. Dist. 3 (Oct. 29, 2004) [hereinafter The Moriah Letter] ("However, FERPA requires that a school respond to reasonable requests for explanations and interpretations of education records, such as answer sheets not accompanied by the question booklets. Thus, a school district should, upon request, provide an opportunity for a parent to review the education records and provide the parent with any explanations and interpretations necessary. This could include the interpretation of standardized test scores, such as reviewing the test questions with the parent.").

[186] The Carroll Letter, *supra* note 183, at 3; *see also* The Moriah Letter, *supra* note 184.

[187] The Carroll Letter, *supra* note 183, at 3; *see also* The Moriah Letter, *supra* note 184.

[188] The Carroll Letter, *supra* note 183, at 3; *see also* The Moriah Letter, *supra* note 184.

[189] The Carroll Letter, *supra* note 183, at 3; *see also* The Moriah Letter, *supra* note 184.

[190] Letter from Mike Olsen to Sen. Richard Blumenthal et al., *supra* note 39 (explaining that Proctorio provides exam administrators with raw video footage).

[191] 20 U.S.C. § 1232g(a)(1)(A) ("Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made.").

vendors' valuable intellectual property.[192] As a result, they may contend that FERPA's right of access does not extend this far or that a student's request for an explanation of automated proctoring flags and suspicion scores is not "reasonable."[193]

But FERPA's legislative history and agency interpretation suggest otherwise—schools (and the vendors who maintain student information on their behalf) must give students access to enough information to be able to assess and challenge the accuracy of information in their education record. Senator James Buckley explicitly sponsored FERPA to prevent erroneous, biased, or unfounded allegations from limiting students' future prospects.[194]

The ED's interpretation of FERPA supports student access to automated proctoring results and rationales. In a FERPA resolution letter, the ED noted that the statute requires schools to provide access to not only test answers but also explanations and interpretations of information in students' education records.[195] This might require "showing the parent the test question booklet, reading the questions to the parent, or providing an interpretation for the responses in some other manner adequate to inform the parent."[196] In other words, required access extends not only to assessment results but also to the tools, criteria, and rationale supporting a student's assessment.

In the context of online proctoring, analogous access would require students to have enough information to assess whether OPT reports reflect accurate flags and scores for suspicious behavior, as well as whether vendors' records contain "inappropriate" data. Students would need to evaluate OPTs' algorithmic inferences to be able to

---

[192] In 2014, for example, Nevada's Department of Education refused to give a father access to data about his children collected by the state. At the time, the state uploaded and stored more than 800 data points daily on each public-school student. The Department had not designed the database for "student-level inspection," and creating a system to produce a report would cost over $10,000. Letter from Dale King, Director, U.S. Dep't of Educ., Fam. Pol'y Compliance Off., to Dale A.R. Erquiaga, Superintendent of Pub. Educ., Nevada Dep't of Educ. (July 28, 2014), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Letter%20to%20Erquiaga%20072814.pdf.

[193] Vendors may also claim trade secret protection, as analytics companies have done in other contexts. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018).

[194] Zeide, *supra* note 163.

[195] The Carroll Letter, *supra* note 183, at 3.

[196] *Id.*

determine whether the information in their records is inaccurate, is misleading, or contains "inappropriate" content.[197]

Vendors would have to provide parents with more than just a log of activity and flags. Students would also need to examine the underlying data, algorithmic model, and the rationale for algorithmic inferences to assess the accuracy of specific determinations and whether the suspicion score and other aspects of OPT reports are misleading.

3. FERPA's Additional Rights to Challenge, Amend, and Annotate

FERPA's expansive right of explanation is supported by three additional rights: contestation, amendment, and annotation. Schools must provide students with the opportunity to challenge information in their education records.[198] Schools must hold a hearing upon request so that students can challenge the content of their education records, in order to ensure that the records are not "inaccurate, misleading, or otherwise in violation of the privacy rights of students."[199] They must amend information determined to be inaccurate, misleading, or inappropriate. Students who lose this hearing can place a statement in the record setting forth their perspective on the contested information.[200] The annotation must be shared whenever schools disclose the relevant underlying information.[201] The rights of inspection

---

[197] 20 U.S.C. § 1232g(a)(1)(A); 34 C.F.R. § 99.10(a) (2022) (establishing the right to inspect and review"); 34 C.F.R. § 99.10(c) (establishing that schools must "respond to reasonable requests for explanations and interpretations of the records"); 20 U.S.C. § 1232g(a)(2); 34 C.F.R. § 99.20(a) (establishing the right to request an amendment and to a hearing to challenge inaccurate, misleading, or inappropriate information in students' education records); 34 C.F.R. § 99.21(b)(2) (establishing the right to insert a written explanation of record contents that schools refuse to amend and have such explanation disclosed with the relevant information).

[198] 20 U.S.C. § 1232g(a)(2); 34 C.F.R. § 99.21(b)(2). The regulation's text echoes FERPA's text, stating that the right includes the opportunity to correct or delete "any such inaccurate, misleading or otherwise inappropriate data contained therein." *Id.*

[199] 20 U.S.C. § 1232g(a)(2).

[200] *Id.*

[201] *Id.*; 34 C.F.R. § 99.21(b)(2) ("If the school does not find the information inaccurate, misleading, or otherwise in violation of the privacy rights of the student, parents have the right to place a statement in the record 'commenting on the contested information in the record or stating why he or she disagrees with the decision of the agency or institution, or both.'"). This statement must be disclosed whenever the school discloses a portion of the record to which the statement relates. 34 C.F.R. § 99.21(c).

and review and their related rights are not subject to the same exceptions as the statute's right of consent.[202] These rights promote one of FERPA's core purposes—to prevent erroneous, biased, or unfounded allegations from limiting students' future prospects.[203]

Students may also be able to use FERPA hearings to challenge the propriety of the breadth, depth, and detail of information that OPTs collect in their comprehensive surveillance of students in intimate spaces. Although FERPA's regulations do not elaborate on the details of what information would be "otherwise in violation of students' privacy rights," the statute explicitly includes education records that contain "inappropriate data."[204] This implies that inappropriate data in students' education records is "otherwise in violation" of their privacy rights.

Students can't use FERPA's amendment rights to appeal school officials' substantive decisions like grades, evaluations, and disciplinary determinations.[205] They can, however, challenge information that may be inaccurate, including "non-substantive factual errors."[206] Schools and vendors would likely argue that students should not be able to challenge automated proctoring inferences because they are substantive decisions.

However, here, vendors' assertions that they only offer decision support works in students' favor. If, in fact, OPTs simply provide information for schools to act on, then students challenging the accuracy of cheating flags and suspicion scores would not be challenging schools' decisions but rather the underlying data that

---

[202] Exceptions to the right to inspect and review orient around certain content, such as letters of recommendations. 34 C.F.R. § 99.12.

[203] Zeide, *supra* note 163. In many cases, students will not prevail in school hearings because the school officials may be reviewing their own decisions. *See* Fanna Gamal, *The Private Life of Education*, 75 STAN. L. REV. 1315, 1319-20 (2023).

[204] 20 U.S.C. § 1232g(a)(2) (establishing the right to correct or delete "any such inaccurate, misleading or otherwise inappropriate data contained therein").

[205] U.S. DEP'T OF EDUC., STUDENT PRIV. POL'Y OFF., SPPO-21-04, A PARENT GUIDE TO THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT GUIDANCE 2 (2021), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/A%20parent%20guide%20to%20ferpa_508.pdf ("[A] school is not required by FERPA to afford a parent the right to seek to change substantive decisions made by school officials, such as substantive decisions made in the context of grades given to a student based on their performance, other evaluations of the student's performance, or disciplinary decisions."); U.S. DEP'T OF EDUC., THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT: GUIDANCE FOR ELIGIBLE STUDENTS 2 (2020), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents.pdf ("[FERPA] may not be used to challenge a grade, an opinion, or a substantive decision made by a school about an eligible student.")

[206] U.S. DEP'T OF EDUC., STUDENT PRIV. POL'Y OFF., *supra* note 205.

schools relied on to make those determinations. They are less like grades or suspensions and more like incorrect data entries.

4. The Agora Letter's Option to Opt Out

Schools that do not provide access to this information deny students their right to access under FERPA. Vendors refusing to supply this information to students or schools upon request are also likely to violate the official exception's "direct control" requirement.[207]

However, students have historically had little recourse for schools' FERPA violations. The statute creates a high threshold for enforcement, requiring schools to have a "policy or practice" of noncompliance before ED seeks to withdraw federal funds. The Department also tries to bring schools into compliance before moving forward with enforcement. But, again, schools would have to repeatedly deny students access to prompt FERPA enforcement.[208]

However, students now have additional leverage to force schools (and vendors) to comply with FERPA's requirements based on the Agora letter, a resolution letter that clarified that students can opt out of education technologies that require them to waive their FERPA rights.[209] Published in 2017, the letter responds to a FERPA complaint filed against the Agora Cyber Charter School, a completely virtual K–12 school.[210]

Agora required parents to consent to terms of service used by one of its technology vendors, K12.[211] These terms granted the vendor "world-wide, perpetual, royalty free and non-exclusive license(s)" over information students posted to the platform, including "all information,

---

[207] Letter from Dale King, Director, U.S. Dep't of Educ., Fam. Pol'y Compliance Off., to Agora Cyber Charter Sch. (Nov. 2 2017) 6 [hereinafter The Agora Letter], https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Agora%20Findings%20letter%20FINAL%2011.2.17.pdf. ED found the Agora School had not violated FERPA's direct control requirements since the parent's complaint was filed before the Department issued guidance on direct control in 2014 and 2015. *Id.* However, the letter implies that ED will impose more stringent standards in the future. *Id.* at 6–7.

[208] If ED finds that a third party rediscloses covered information in violation of FERPA's disclosure requirements, it can prohibit a school from sharing information with the party for at least five years. 34 C.F.R. § 99.67(c) (2022). However, this power doesn't extend to violations of the statute's right to inspect and review.

[209] The Agora Letter, *supra* note 207, at 4–5.

[210] *Id.*

[211] *Id.* at 6.

data, text, software, music, sound, photographs, graphics, video, messages, tags or other materials."[212] These terms gave K12 and its affiliates and licensees the right to "use, reproduce, display, perform, adapt, modify, distribute, have distributed, and promote the content in any form, anywhere and for any purpose."[213] ED found that this expansive language gave the vendor "near universal use and distribution" rights over students' personally identifiable student information.[214]

The letter noted that these terms would permit K12 to post students' personally identifiable information online, share it with future employers, or distribute it to any third party to be used for any purpose and further disclosed without limitation.[215] These use and disclosure rights effectively waived FERPA's protections against unauthorized disclosure of covered information.[216] Schools cannot require students to waive their FERPA rights as a condition of receiving an education.[217] Accordingly, Agora could not force students to use the K12 software.[218]

While the Agora letter involves FERPA's right of consent, its findings should also apply to the statute's right of access.[219] Accordingly, schools cannot require students to use a specific proctoring technology if vendors do not satisfy the right's requirements, including access, explanation, contestation, and annotation. If educators continued to use a technology that did not provide adequate access, ED could also find

---

[212] *Id.* at 5–6.
[213] *Id.* (emphasis omitted).
[214] *Id.*
[215] *Id.* at 6.
[216] *Id.*
[217] *Id.* at 4–5 ("[I]n no circumstances does FERPA permit an educational agency or institution to require a student to waive the rights and protections afforded under FERPA in order to apply for or receive educational training or services.") (citation omitted).
[218] *Id.*; Dian Schaffhauser, *FERPA Finding Reminds Schools to Review Terms of Service*, The JOURNAL (Jan. 30, 2018), https://thejournal.com/articles/2018/01/30/ferpa-finding-reminds-schools-to-review-terms-of-service.aspx; Jim Siegl, *Plagiarism, Precedence and the Agora Letter*, PRIVACY IS HARD (Jan. 19, 2018), https://privacyishard.net/plagiarism-precedence-and-the-agora-letter/.
[219] The Agora Letter, *supra* note 207, at 4–5 ("[I]n no circumstances does FERPA permit an educational agency or institution to require a student to waive the rights and protections afforded under FERPA in order to apply for or receive educational training or services.") (citation omitted).

that the school had a "policy or practice" of FERPA violations sufficient to trigger enforcement.[220]

Using FERPA to force algorithmic accountability is a powerful tool to promote due process in individual cases. Enough of these individual challenges might lead vendors to improve their practices overall.

5. The Insufficiency of Individual Contestation

Individual exercise of FERPA rights is an imperfect solution at best. Exercising FERPA rights is time-consuming and resource-intensive for parents, students, schools, and vendors.[221] Algorithmic opacity—the notorious "black box" of AI—may make it difficult for companies to surface the inputs and rationales for decisions necessary for students to evaluate whether the information is accurate and appropriate.[222]

This can be an expensive proposition. However, schools (and therefore vendors) cannot condition FERPA access on payment of prohibitive fees.[223] Many companies may already deploy technology/systems that perform similar tasks to comply with their obligations under the General Data Protection Regulation (GDPR).[224] Even with vendors providing access to the relevant information, ex post review of algorithmic inferences is challenging to do in practice given

---

[220] *See* 20 U.S.C. § 1232g(a)(1)(A)–(B), (b)(1)–(2) (stating that funds shall not be made available under any applicable program to educational agencies or institutions that have a policy or practice of denying or effectively preventing the exercise of rights assured under FERPA or of permitting the release of educational records without written consent).

[221] Vendors may have to develop tools to retrieve and permit parents to access specific student records without compromising other students' privacy.

[222] *See, e.g.*, Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, BIG DATA & SOC'Y, Jan.–June 2016, at 1; Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014).

[223] Nevada's Department of Education originally informed a father that he would have to bear the $10,000 cost of creating a system that would provide student-level data for his daughter. Federal authorities disagreed, stating that the Department could not condition access by charging students or parents prohibitive fees. Letter from Dale King to Dale A.R. Erquiaga, *supra* note 192.

[224] Regulation 2016/679, of the European Parliament and of 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

algorithmic opacity and complexity. Experts disagree about what constitutes algorithmic accuracy and fairness.[225] Parents and school officers will not only have to agree upon what metric of accuracy to apply but also understand the complexities of AI in order to assess OPT inferences. Just as in the context of GDPR and analogous ex post constatation regimes, relying on individuals to ensure algorithmic accountability is insufficient to promote systemic reform.[226]

B. Biometric Privacy Laws

1. State Student Biometric Privacy Laws

Several states have passed laws precluding K–12 public schools from collecting students' biometric data.[227] OPTs' facial detection and analysis tools fall squarely within their prohibited practices. While some states permit parents to consent to biometric data collection,[228] it is unclear whether schools obtained this consent prior to implementing OPTs. Two states prohibit schools from collecting biometric information entirely, with no exception for parental consent. A Florida

---

[225] *See, e.g.*, Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; WILLIAM DIETERICH ET AL., NORTHPOINTE INC., COMPAS RISK SCALES: DEMONSTRATING ACCURACY EQUITY AND PREDICTIVE PARITY (2016), https://go.volarisgroup.com/rs/430-MBX-989/images/ProPublica_Commentary_Final_070616.pdf; Julia Angwin & Jeff Larson, *ProPublica Responds to Company's Critique of Machine Bias Story*, PROPUBLICA (July 29, 2016, 11:56 AM), https://www.propublica.org/article/propublica-responds-to-companys-critique-of-machine-bias-story.

[226] *See* Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 1957, 1984–88 (2021) (detailing recent scholarship supporting and critical of due process as a mechanism for regulating artificial intelligence); Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (2019).

[227] *See, e.g.*, 105 ILL. COMP. STAT. 5/34-18.34(b)(1) (2022); LA. STAT. ANN. § 17:100.8(B)(2) (2023); ARIZ. REV. STAT. ANN. § 15-109 (2023) (barring collection of biometric data absent prior parental consent); FLA. STAT. § 1002.222(1)(a) (2023) (prohibiting schools and districts from collecting, obtaining, or retaining any student biometric information including fingerprints, hand scans, retina or iris scans, voice prints, and facial geometry scans); N.Y. STATE TECH. LAW § 106-b (McKinney 2023) (banning the state education commissioner from approving elementary and secondary schools' use or purchase of biometric identifying technology until July 2022 or when the State Education Department promulgates a report addressing the legislature's concerns).

[228] *See* 105 ILL. COMP. STAT. 5/34-18.34(b)(1); LA. REV. STAT. ANN. § 100.8(B)(2); ARIZ. REV. STAT. ANN. § 15-109 (barring collection of student biometric data absent prior parental consent).

law passed in 2014 bars schools and districts from collecting, obtaining, or retaining any student biometric information, including facial geometry.[229] New York passed a law in 2021 suspending the use of biometric identifying technology in elementary and secondary schools until July 2022.[230] However, neither law offers students a private right of action nor provides specific enforcement mechanisms. The Florida statute hasn't been enforced despite schools' public use of students' biometric data.

2. Illinois's Biometric Information Privacy Act

Some Illinois students could recover damages from OPT vendors for violations of the state's BIPA.[231] BIPA regulates private entities' collection, use, safeguarding, and storage of biometric data of Illinois state residents.[232] The statute imposes stringent written notice and consent requirements, data retention and disclosure limits, and security measures; it also prohibits companies from profiting from biometric data.[233]

Specifically, BIPA requires companies to provide written notice to data subjects as to what biometric information the vendor is collecting, for what purpose, and for how long.[234] Covered entities must have a public written policy establishing a retention schedule and guidelines for destroying covered information within three years of the data subject's last interaction with a company or once the company has satisfied the original purpose for collection, whichever comes first.[235] They must obtain written consent to collect or redisclose biometric

---

[229] FLA. STAT. § 1002.222(1)(a) (prohibiting schools and districts from collecting, obtaining, or retaining any student biometric information including fingerprints, hand scans, retina or iris scans, voice prints, and facial geometry scans).
[230] N.Y. STATE TECH. LAW § 106-b (banning the state education commissioner from approving elementary and secondary schools' use or purchase of biometric identifying technology until July 2022 or when the State Education Department promulgates a report addressing the legislature's concerns).
[231] 740 Ill. Comp. Stat. 14.
[232] *Id.* 14/15(a) (applying the statute to private entities); *Id.* 14/10 ("'Private entity' means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency.").
[233] *Id.* 14/15.
[234] *Id.*
[235] *Id.*

data.[236] Finally, organizations must use reasonable standards of care to prevent unauthorized access to stored biometric information.[237] Unlike the student biometric privacy laws described above, BIPA includes a private right of action that allows students to recover actual and liquidated damages for violations.[238]

Several students have already filed BIPA claims against OPTs and private universities based on test administration practices during the pandemic.[239] These suits allege that the vendor or school failed to

---

[236] *Id.*
[237] *Id.*
[238] *Id.* 14/20.
[239] Powell v. DePaul Univ., No. 21 C 3001, 2022 WL 16715887 (N.D. Ill. Nov. 4, 2022); Duerr v. Bradley Univ., 590 F. Supp. 3d 1160 (C.D. Ill. 2022); Doe v. Elmhurst Univ., No. 2020 L 1400 (Ill. Cir. Ct. Nov. 18, 2021); Fee v. Ill. Inst. of Tech., No. 21-cv-02512, 2022 U.S. Dist. LEXIS 125581 (N.D. Ill. July 15, 2022); Patterson v. Respondus, Inc., No. 20 C 7692, 2022 U.S. Dist. LEXIS 51991 (N.D. Ill. Mar. 23, 2022); Complaint at 2, Thakkar v. ProctorU Inc., No. 21-cv-02051, (C.D. Ill. Mar. 12, 2021), ECF No. 1 (alleging that ProctorU violated BIPA by failing to provide the requisite data retention and destruction policies and failed to properly store, transmit, and protect from disclosure these biometrics); Complaint at 1–2, Clarke v. Examity, Inc., No. 21-cv-02081, (N.D. Ill. Apr. 16, 2021), ECF No. 1 (alleging that Examity violated BIPA by failing to provide the requisite data retention and destruction policies and failed to provide the specific purpose and length of term for biometrics were being collected, stored, and used); Complaint at 4, Hinds v. Respondus, No. 21-cv-07692, (N.D. Ill. Dec. 23, 2020) ECF No. 1 (alleging that Respondus violated BIPA by failing to provide the requisite data retention; failing to obtain students' written informed consent for collecting, using, and disclosing students' biometrics; and profiting from students' biometrics through contracts with educational institutions); Complaint at 4, Bridges v. Respondus, No. 21-cv-01785, (N.D. Ill. Apr. 2, 2021) ECF No.1 (alleging that Respondus violated BIPA by failing to provide the requisite data retention; failing to obtain students' written informed consent for collecting, using, and disclosing students' biometrics; and profiting from students' biometrics through contracts with educational institutions); Complaint at 4, Duerr v. Bradley Univ., No. 21-cv-01096, (C.D. Ill. Mar.18, 2021) ECF No.1-1 (alleging that university violated BIPA through Respondus by failing to provide the requisite data retention and failing to obtain students' written informed consent for collecting, using, and disclosing students' biometrics); Complaint at 4, Doe v. DePaul Univ., No. 2021-CH-01027 (Ill. Cir. Ct. Mar. 3, 2021) (alleging that university violated BIPA through Respondus by failing to provide the requisite data retention and failing to obtain students' written informed consent for collecting, using, and disclosing students' biometrics); Complaint at 4, Doe v. Illinois Inst. of Tech., No. 21-cv-02512, (N.D. Ill. May 10, 2021) ECF No. 1-1 (alleging that institution violated BIPA through Respondus by failing to provide the requisite data retention and failing to obtain students' written informed consent for collecting, using, and disclosing students' biometrics); Complaint at 1, Doe v. Nw. Univ., No. 21-cv-01579, (N.D. Ill. Mar. 22, 2021) ECF No. 1 (alleging that university violated BIPA through remote proctoring companies–Respondus and Examity—by failing to obtain students' written and informed consent for collecting, using, and disclosing students' biometrics); Complaint

provide sufficient notice about collecting and retaining students' biometrics, invalidating any prior consent.[240]

Students' most substantial claims involve the Respondus proctoring system.[241] They allege that the company did not explicitly disclose its use of facial recognition and analysis technologies or clearly describe its retention practices until it updated its terms of service in January 2021.[242] Other complaints have a strong argument that ProctorU did not implement reasonable security measures, as demonstrated by a data breach of nearly 500,000 student records in July 2020.[243] However, BIPA excludes "financial institutions" covered by the Gramm-Leach-Bliley Act (GLBA).[244] Following the FTC and ED interpretation of GLBA, several courts have found that this exemption applies to higher education institutions that make and administer

---

at 15, Veiga v. Respondus Inc., No. 21-cv-02620 (N.D. Ill. May 14, 2021) ECF No. 1 (alleging that Respondus violated BIPA by failing to provide the requisite data retention schedule and guidelines); Complaint at 2, Frederick v. ExamSoft Worldwide, Inc., No. 21-cv-02190 (N.D. Ill. Apr. 22, 2021) ECF No. 1-2 (alleging that ExamSoft violated BIPA by failing to provide the requisite data retention schedule and guidelines); Complaint at 12, Lam Andrew v. Verificient Tech., No. 2021-CH-00758 (Ill. Cir. Ct. Feb. 17, 2021) (alleging that Proctortrack violated BIPA by failing to employ a reasonable standard of care in storing, transmitting, and protecting from disclosure biometric identifiers and biometric information)

[240] *See, e.g.*, Powell v. DePaul Univ., No. 21 C 3001, 2022 WL 16715887 (N.D. Ill. Nov. 4, 2022); Duerr v. Bradley Univ., 590 F. Supp. 3d 1160 (C.D. Ill. 2022) ; Doe v. Elmhurst Univ., No. 2020 L 1400 (Ill. Cir. Ct. Nov. 18, 2021); Fee v. Ill. Inst. of Tech., No. 21-cv-02512, 2022 U.S. Dist. LEXIS 125581 (N.D. Ill. July 15, 2022); Patterson v. Respondus, Inc., No. 20 C 7692, 2022 U.S. Dist. LEXIS 51991 (N.D. Ill. Mar. 23, 2022).

[241] Complaint, Hinds, *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Bridges, *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Duerr, *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Doe v. DePaul Univ., *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Doe v. Ill. Inst. of Tech., *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Nw. Univ., *supra* note **Error! Bookmark not defined.**, at 1; Complaint, Veiga, *supra* note **Error! Bookmark not defined.**, at 15.

[242] *See, e.g.*, Complaint, Hinds, *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Bridges, *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Duerr, *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Doe v. DePaul Univ., *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Doe v. Ill. Inst. of Tech., *supra* note **Error! Bookmark not defined.**, at 4; Complaint, Nw. Univ., *supra* note **Error! Bookmark not defined.**, at 1; Complaint, Veiga, *supra* note **Error! Bookmark not defined.**, at 15.

[243] Complaint, Thakkar, *supra* note **Error! Bookmark not defined.**, at 2.

[244] 740 ILL. COMP. STAT. 14/25(c) (2022).

student loans.[245] As a result, students can only bring BIPA claims against OPT vendors, private schools that don't offer aid, and professional licensing associations like state bar examiners.

These plaintiffs have a good chance of success, which would provide at least a few students with deserved compensation. BIPA victories would undoubtedly prompt vendors and schools to make the required disclosures and institute consent protocols. They might even deter some Illinois schools from adopting technologies that collect biometric data. But successful BIPA suits are unlikely to prompt meaningful reform—vendors can avoid further liability by merely tweaking their marketing and documentation. Schools and students would just be better informed about vendors' problematic practices.

C. Consumer Protection

Consumer protection laws also offer a way to address OPTs. However, like state student biometric privacy laws, they depend on uncertain regulator enforcement. Prompted by consumer complaints, public outcry, or their own observations, the FTC and state attorneys general could investigate proctoring technology vendors for engaging in unfair or deceptive trade practices in violation of Section 5 of the Federal Trade Commission Act and analogous state consumer protection statutes.[246] Here, however, the FTC would not be acting to protect "students" per se. Since the FTC's jurisdiction applies to commercial entities, its authority would extend to harms inflicted by OPT vendors and the for-profit schools using their products. FTC enforcement would not address individual test-takers' grievances but would instead consider the impact of OPT practices on consumers at large. However, FTC enforcement against any of these entities would effectively set standards across the proctoring industry.

---

[245] *Powell*, 2022 WL 16715887 (finding that a university that participates in federal financial aid programs is a "financial institution" under the Gramm-Leach-Bliley Act, and so exempt from BIPA under the statute's Section 25(c)); Duerr, 590 F. Supp. 3d at 1171 (finding that Bradley University met the GBLA definition of a "financial institution," which includes entities "significantly engaged in financial activities" or "significantly engaged in activities incidental to such financial activities."); Doe v. Northwestern Univ., *supra* note **Error! Bookmark not defined.**; Doe v. Elmhurst Univ., *supra* note **Error! Bookmark not defined.**; Fee v. Ill. Inst. of Tech., *supra* note **Error! Bookmark not defined.**.

[246] While this article considers federal consumer protection enforcement, much of the analysis applies to analogous state statutes.

1. Deceptive Trade Practices

The FTC could find that OPTs engaged in deceptive trade practices by making exaggerated and unsupported claims about their products' abilities to verify student identities, detect academic misconduct, eliminate bias, and reduce cheating overall. Under the FTC Act, a company engages in a deceptive trade practice if it makes a material representation or omission likely to mislead a consumer acting reasonably in the circumstances.[247] These include statements that "lack[] a 'reasonable basis' to support the claims made[.]"[248] The representations must be sufficiently material to affect consumers' decisions related to the product or service.[249]

Although the FTC hasn't explicitly addressed proctoring systems, test-takers made similar allegations that ExamSoft exaggerated the security, accuracy, and reliability of its software used to administer bar exams in 2014.[250] While ExamSoft asserted that its many software glitches had not impacted exam integrity, data indicated a marked decline in the number of people who passed the test and their scores.[251] The company reached a 2.1-million-dollar settlement with test-takers in 2015.[252]

---

[247] 15 U.S.C. § 45(n).

[248] Daniel Chapter One v. F.T.C., 405 F. App'x 505, 506 (D.C. Cir. 2010) (quoting Thompson Med. Co., Inc. v. F.T.C., 791 F.2d 189, 193 (D.C. Cir. 1986)). When an advertiser claims that its product is proven to work—i.e., that its efficacy has been "established"—a reasonable basis for that claim "must consist of the precise type and amount of proof that would satisfy the relevant scientific community." Removatron Int'l Corp., 111 F.T.C. 206, 306 (1988) (citations omitted), enforced, 884 F.2d 1489 (1st Cir. 1989).

[249] Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to Hon. John D. Dingell, Chairman, U.S. House of Representatives, Comm. on Energy & Com. (Oct. 14, 1983), *appended to* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984)).

[250] Complaint and Demand for Jury Trial at 27, Rangi. v. ExamSoft Worldwide, Inc., No. 14-cv-01919 (E.D. Cal. Aug. 15, 2014).

[251] Dan McCue, *Bar Exam Software Firm to Pay $2.1M Settlement*, COURTHOUSE NEWS (May 21, 2015), https://www.courthousenews.com/bar-exam-software-firm-to-pay-2-1m-settlement/; *ExamSoft to Settle Bar Exam Software Glitch Class Action for $2.1 Million*, MORGAN AND MORGAN (May 11, 2015) https://www.forthepeople.com/blog/examsoft-settle-bar-exam-software-glitch-class-action-21-million/.

[252] McCue, *supra* note 251; *ExamSoft to Settle Bar Exam Software Glitch Class Action for $2.1 Million*, *supra* note 251; F.T.C. v. Lumos Labs, No. 3:16-cv-00001, at 8 (N.D. Cal. Jan. 8, 2016), https://www.ftc.gov/system/files/documents/cases/160105lumoslabsstip.pdf.

OPTs may claim their products are sufficiently accurate when used, as vendors intend, for decision support. They might contend that the question is not whether their software accurately detects cheating, but whether it accurately flags *possible* misconduct. Proctorio used this logic to sidestep senators' inquiries about its products' accuracy, stating, "Our software does not make inaccurate determinations about violations of exam integrity because our software does not make any determinations about breaches of exam integrity."[253] But even OPTs used for decision support must meet some minimum threshold for accuracy to support vendors' promises that their products improve upon human proctoring.[254] It is not clear OPTs can meet even that lowered standard.[255]

The FTC's complaint and settlement with Lumosity is instructive.[256] The edtech company claimed that playing its games for ten to fifteen minutes several times a week would delay memory decline, protect against cognitive decline, improve academic and athletic performance, and reduce the effects of conditions ranging from attention-deficit/hyperactivity disorder to post-traumatic stress disorder.[257] The FTC found Lumosity did not have evidence supporting these promises, which would require human clinical testing.[258] It imposed a $50 million judgment.[259]

The FTC could charge OPTs with making similarly unsupported claims about their verification and cheating detection technologies by overstating their accuracy and ability to eliminate "human error [and]

---

[253] Letter from Mike Olsen to Sen. Richard Blumenthal et al., *supra* note 39, at 9 (emphasis omitted).
[254] Coghlan et al., *supra* note 12, at 1592.
[255] *See, e.g.*, Skolnik, *supra* note 90.
[256] F.T.C. v. Lumos Labs, No. 3:16-cv-00001, at 8 (N.D. Cal. Jan. 8, 2016), https://www.ftc.gov/system/files/documents/cases/160105lumoslabsstip.pdf; *Lumosity to Pay $2 Million to Settle FTC Deceptive Advertising Charges for Its "Brain Training" Program*, FED. TRADE COMM'N (Jan. 5, 2016), https://www.ftc.gov/news-events/press-releases/2016/01/lumosity-pay-2-million-settle-ftc-deceptive-advertising-charges.
[257] F.T.C. v. Lumos Labs, No. 3:16-cv-00001, at 8 (N.D. Cal. Jan. 8, 2016), https://www.ftc.gov/system/files/documents/cases/160105lumoslabsstip.pdf; *Lumosity to Pay $2 Million to Settle FTC Deceptive Advertising Charges for Its "Brain Training" Program*, *supra* note 256.
[258] F.T.C. v. Lumos Labs, No. 3:16-cv-00001, at 8 (N.D. Cal. Jan. 8, 2016), https://www.ftc.gov/system/files/documents/cases/160105lumoslabsstip.pdf; *Lumosity to Pay $2 Million to Settle FTC Deceptive Advertising Charges for Its "Brain Training" Program*, *supra* note 256.
[259] F.T.C. v. Lumos Labs, No. 3:16-cv-00001, at 8 (N.D. Cal. Jan. 8, 2016), https://www.ftc.gov/system/files/documents/cases/160105lumoslabsstip.pdf; *Lumosity to Pay $2 Million to Settle FTC Deceptive Advertising Charges for Its "Brain Training" Program*, *supra* note 256.

bias."[260] OPT companies allege that their online proctoring tools can reliably detect signs of cheating and ensure test "integrity."[261] However, it is unclear whether vendors have sufficient empirical evidence to constitute a "reasonable basis" for these claims.[262]

The FTC recently cautioned companies against exactly this kind of hype, warning them not to "exaggerate what [their] algorithm can do or whether it can deliver fair or unbiased results."[263] The agency used the example of a developer claiming that the algorithm provides "100% unbiased hiring decisions," despite training it on data lacking racial or gender diversity.[264] It is telling that Proctorio changed its claims just after the release of this guidance—saying that its software "attempts" to eliminate,[265] not that it definitely "eliminates," human error and bias.[266] The website makes no claims about reducing bias today.

The FTC might also find that vendors misstated specifics about their data practices, such as whether they use facial detection or facial

---

[260] PROCTORIO, https://proctorio.com (last visited Oct. 19, 2021) [https://web.archive.org/web/20190126031131/https://proctorio.com/].

[261] *Respondus Monitor: Protecting the Integrity of Online Exams*, RESPONDUS, https://web.respondus.com/respondus-monitor-protecting-the-integrity-of-online-exams/ (last visited Nov. 19, 2022) ("But how do you ensure the integrity of online exams and prevent cheating? The answer is with LockDown Browser and Respondus Monitor."); *Prevention*, PROCTORU (2020), https://www.proctoru.com/integrity-in-action ("Our job is to deter and prevent any breach of integrity."); *A Comprehensive Learning Integrity Platform*, PROCTORIO (2020), https://Proctorio.com/ ("Using state-of-the-art technology and end-to-end data security, Proctorio ensures the total learning integrity of every assessment, every time."); *Test-taker FAQs*, EXAMITY (2020), https://www.examity.com/test-takers/ ("[Examity] provides teachers, schools and students with the tools they need to prevent cheating and to preserve integrity."); *Provide Flexibility and Protect Your Reputation*, HONORLOCK (2020), https://honorlock.com/; *What is Academic Integrity*, HONORLOCK (2021), https://honorlock.com/blog/what-is-academic-integrity/ ("Honorlock upholds academic integrity with remote proctoring that's monitored by AI and reviewed by humans.").

[262] *See supra* Section I.B.2–.4.

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

[264] *Id.*

[265] PROCTORIO, *supra* note 59.

[266] PROCTORIO, *supra* note 260.

recognition technologies.[267] However, such technicalities may not be sufficiently material to consumers to support a finding of deception.

2. Unfair Trade Practices

The FTC might also find that vendors' unsupported claims about their products' capabilities constitute unfair trade practices. The unfairness prong of the FTC Act prohibits conduct causing or likely to cause substantial injury to consumers, where that injury is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or to competition.[268] Students cannot reasonably avoid using proctoring tools mandated by their schools. Those excluded from exams or accused of cheating should be able to show a substantial injury.[269]

The agency signaled that it may take a more aggressive stance to enforce fair deployment of automated decision-making and artificial intelligence.[270] Recent guidance emphasizes that vendors need to substantiate claims about their algorithmic tools and test both inputs and outputs for discriminatory impact.[271] Accordingly, the FTC could find that algorithmic bias renders automated proctoring technologies

---

[267] *Complaint and Request for Investigation*, *supra* note 36 (alleging proctoring companies deceived consumers about their use of facial recognition technologies and data minimization practices). Proctorio and Honorlock, for example, state that they use "facial detection," not "facial recognition" tools. *See Frequently Asked Questions*, PROCTORIO, https://proctorio.com/frequently-asked-questions (last visited 2020); *Student Privacy FAQ*, HONORLOCK, https://honorlock.com/studentprivacy/#faq (last visited 2020). FTC guidance has previously described facial detection as a subset of "facial recognition" technologies. Lesley Fair, *Facing the Facts About Facial Recognition*, FED. TRADE COMM'N (Jan. 11, 2021), https://www.ftc.gov/business-guidance/blog/2021/01/facing-facts-about-facial-recognition. Respondus's failure to disclose that it engaged in facial analysis at all is a more serious omission. *See supra* Section II.B.

[268] 15 U.S.C. § 45(n).

[269] "Substantial injury" must be more than trivial and can include monetary, economic, health-related, or other types of tangible harms. *Id.*; Letter from Michael Pertschuk, Chairman, Fed. Trade Comm'n, to Hon. Wendell H. Ford, Chairman, Comm. on Com., Sci, & Transp., Consumer Subcomm. (Dec. 17, 1980), *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1073 (1984) [hereinafter FTC Unfairness Policy]; Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439, 482–84 (2020).

[270] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N: BUS. BLOG (Apr. 8, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms; Jillson, *supra* note 263; *see also* Rebecca Kelly Slaughter et al., *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J.L. & TECH. 1, 13–14 (2020).

[271] Smith, *supra* note 270; Slaughter et al., *supra* note 270.

unfair if, for example, their software disproportionately flags neurodivergent students as suspicious.[272] The cost/benefit prong of the unfairness test is less clear cut. The FTC considers not only the costs and benefits to individual consumers but to society as a whole when determining whether a practice is "injurious in its net effects."[273] It can also take "established public policies" into account when determining whether a given practice is unfair.[274]

OPTs' practices also fall short of industry standards, including the Association of Test Publishers' Best Practices for Artificial Intelligence in Testing[275] and the Standards for Educational and Psychological Testing promulgated by the American Educational Research Association, the American Psychological Association, and the National Council on Measurement in Education.[276] Both documents exhort the importance of fairness, non-discrimination, privacy, accuracy, human review of automated decisions, and a right of appeal for consequential decisions.[277] The American Test Publishers' Association explicitly states that automated cheating detection systems without live human oversight do not meet its definition of "proctoring."[278]

These industry standards echo an emerging consensus about the ethical use of artificial intelligence. More than sixty prominent entities

---

[272] Jillson, *supra* note 263.

[273] FTC Unfairness Policy, *supra* note 269, at 1073 (explaining that, in evaluating the costs, the FTC considers "not only the costs to the parties directly before the agency, but also the burdens on society in general"); Hirsch, *supra* note 269, at 482–84.

[274] There is also the confounding question of how to define "fair." Deirdre K. Mulligan et al., *This Thing Called Fairness: Disciplinary Confusion Realizing a Value in Technology*, 3 PROC. ACM ON HUMAN-COMPUTER INTERACTION 1 (2019).

[275] INT'L PRIVACY SUBCOMM. OF THE ATP SECURITY COMM., *supra* note 45, at 2.

[276] *Id.*; AM. EDUC. RSCH. ASS'N ET AL., STANDARDS FOR EDUCATIONAL AND PSYCHOLOGICAL TESTING (2014), https://www.testingstandards.net/uploads/7/6/6/4/76643089/9780935302356.pdf (emphasizing the importance of fairness, non-discrimination, privacy, accuracy, human review of automated decisions, and providing a right of appeal of consequential decisions in testing).

[277] INT'L PRIVACY SUBCOMM. OF THE ATP SECURITY COMM., *supra* note 45; AM. EDUC. RSCH. ASS'N ET AL., *supra* note 276 (emphasizing the importance of fairness, non-discrimination, privacy, accuracy, human review of automated decisions, and providing a right of appeal of consequential decisions in testing).

[278] ATP-NCTA PROCTORING COMM., PROCTORING BEST PRACTICES: ASSOCIATION OF TEST PUBLISHERS AND NATIONAL COLLEGE TESTING ASSOCIATION 46 (2015) (stating that "record and review" online systems without live human oversight does not meet its definition of "proctoring").

have promulgated ethical AI principles in the past several years that feature many of the same central components: privacy, accountability, safety and security, transparency and explainability; fairness and non-discrimination; human control of technology; professional responsibility; and promotion of human values.[279] Similar values are foundational in the GDPR and reflected in proposed and enacted state laws in the United States.[280] As discussed above, pandemic proctoring violates many of these standards.[281] However, these industry and institutional principles are not widely recognized in the statutes, common law, or judicial decisions that the FTC considers "established public policy."[282]

In sum, vendors' flawed proctoring technology and unsupported marketing claims can support aggressive enforcement, but the success of consumer protection claims will depend on the specific evidence at hand and, more significantly, the FTC's broader policies and priorities.

D. Civil Rights Claims

The disproportionate impact of OPTs on marginalized students raises the possibility that students can use antidiscrimination law to obtain individual redress and prompt proctoring industry reform. The automated components of proctoring technologies may have a disproportionately negative impact on protected classes of students—

---

[279] Jessica Fjeld et al., *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*, SSRN ELEC. J. (Berkman Klein Ctr. for Internet & Soc'y Rsch. Publ'n Series, Rsch. Publ'n No. 2020-1, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482. The United States and the G20 have adopted the Organisation for Economic Co-operation and Development's "Principles on AI." *Recommendation of the Council on Artificial Intelligence*, OECD.AI POL'Y OBSERVATORY, https://oecd.ai/en/ai-principles (last visited Nov. 19, 2022) (including "freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, [and] fairness"; accountability for the proper functioning of the AI system; "transparency and responsible disclosure," including "easy-to-understand information on the factors, and the logic that served as the basis for [any] prediction, recommendation or decision."); *Universal Guidelines for Artificial Intelligence,* THE PUB. VOICE (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/ (including rights to transparency, assessment, and accountability, accuracy, reliability, validity, and fairness).

[280] GDPR art. 21 ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."). An organization using automated processing must provide a "clear and separate" notice of the automated process and the individual's right to object.

[281] *See supra* Part I.

[282] FTC Unfairness Policy, *supra* note 269, at 1070, 1074–76 (referring to "statute[s], common law," and "judicial decisions" as sources of established public policy).

particularly those with dark skin, those who wear religious headwear, or those with disabilities.[283] Commenters understandably chastise the technology as racist and discriminatory.[284] But as with other incidences of algorithmic bias,[285] it will be difficult for students to meet the daunting standards required to establish legal discrimination in violation of the Equal Protection Clause, Title VI of the Civil Rights Act of 1964 ("Title VI"), Title II of the Americans with Disabilities Act of 1990 (ADA), or Section 504 of the Rehabilitation Act of 1973 ("Section 504").[286]

1. Equal Protection Clause

The Equal Protection Clause establishes that no state may "deny to any person within its jurisdiction the equal protection of the laws."[287] This well-known section of the Fourteenth Amendment helps protect citizens from arbitrary and discriminatory state action. However, complainants in the education context must show discriminatory intent to establish an equal protection violation.[288] Since the adoption of

---

[283] Coghlan et al., *supra* note 12.
[284] *See, e.g.*, Asher-Schapiro, *supra* note 24; Morse, *supra* note 24; Cahn et al., *supra* note 25; Feathers, *supra* note 26; Brown, *supra* note 95.
[285] *See, e.g.*, Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 920–21 (2017) ("In order for claimants to diagnose whether statistical bias has infected an algorithm, they would need access to the training data and the underlying model. The claimants would have to trace how the data miners collected the data, determine what populations were sampled, and audit the records for errors."); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016); Amit Datta et al., *Discrimination in Online Personalization: A Multidisciplinary Inquiry*, 81 PROC. MACH. LEARNING RSCH. 20 (2018); MIRANDA BOGEN & AARON RIEKE, UPTURN, HELP WANTED: AN EXAMINATION OF HIRING ALGORITHMS, EQUITY, AND BIAS (2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf; McKenzie Raub, *Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices*, 71 ARK. L. REV. 529 (2018).
[286] Bar exam test-takers cannot take advantage of the education-specific discrimination statutes discussed below. Further, they cannot raise discrimination claims under Title VII of the Civil Rights Act of 1964, since licensing tests have been found to lie outside that statute's protection. *See* Joan W. Howarth, *The Professional Responsibility Case for Valid and Nondiscriminatory Bar Exams*, 33 GEO. J. LEGAL ETHICS 931, 937–47 (2020) (describing decisions immunizing bar examiners from Title VII requirements).
[287] U.S. CONST. amend. XIV, § 1.
[288] *See* Amy B. Cyphert, *Tinker-ing with Machine Learning: The Legality and Consequences of Online Surveillance of Students*, 20 NEV. L.J. 457, 496–97 (2020).

proctoring technologies is not explicitly discriminatory, there is no obvious support for an equal protection claim.

2. Title VI Discrimination

Aggrieved students could file a complaint with ED's Office for Civil Rights (OCR) alleging that proctoring technologies frequently misidentify or fail to detect dark skin, leading to a disproportionately negative impact on students of color. However, the agency is not likely to find legally actionable discrimination. OCR often resolves its investigations informally by facilitating a resolution between the parties and executing a resolution agreement before issuing any final determination.[289] This could still have a significant impact on vendor and school practices if OCR implied a likely violation of students' civil rights. However, the overall inaccuracy of OPT's automated technologies across all groups may make it difficult to establish a sufficient disparate impact on protected classes. Finally, schools also have a strong defense that using OPTs during pandemic school closures was an educational necessity to ensure academic integrity and that less discriminatory alternatives were not available or feasible.

Title VI of the Civil Rights Act of 1964 prohibits discrimination based on race, color, and national origin by any program or activity receiving federal financial assistance.[290] Specifically, schools cannot exclude students from participating in their programs or activities on the basis of race, color, or national origin.[291] Unlike Title VII, the corresponding guarantee of civil rights in employment,[292] Title VI only provides a private right of action for intentional discrimination.[293] As a result, individuals seeking to challenge an education practice with a disparate impact must rely on OCR enforcement.[294] In Title VI

---

[289] U.S. DEPT. OF EDUC., OFF. FOR C.R., CASE PROCESSING MANUAL §§ 201, 302 (2020).
[290] 42 U.S.C. §§ 2000d to 2000d-4a.
[291] *See* 42 U.S.C. § 2000d; 34 C.F.R. § 100.3 (2022).
[292] Civil Rights Act of 1964, Title VII, 42 U.S.C. §§ 2000e to 2000e-17.
[293] Alexander v. Sandoval, 532 U.S. 275, 285 (2001) ("It is clear now that the disparate-impact regulations do not simply apply § 601—since they indeed forbid conduct that § 601 permits—and therefore clear that the private right of action to enforce § 601 does not include a private right to enforce these regulations.").
[294] *See* 34 C.F.R. § 100.3(b)(2) (2022); U.S. Dep't of Educ., Off. for C.R. & U.S. Dep't of Just., C.R. Div., Dear Colleague Letter on the Nondiscriminatory Administration of School Discipline 11 (2014),

administrative investigations, the agency itself bears the evidentiary burden for both interrogating allegations of discrimination and uncovering less discriminatory alternatives where applicable.[295]

OCR primarily enforces Title VI through non-adversarial resolution of complaints.[296] It first attempts to facilitate resolution between the parties. If negotiation fails, it conducts an administrative investigation that frequently concludes with a voluntary resolution between the school and OCR that is memorialized with a "resolution letter."[297] It is only in rare instances that OCR cannot negotiate or secure compliance, which would prompt either an administrative proceeding resulting in the termination of federal funds or the referral of a complaint to the Department of Justice for litigation.[298]

Many substantive aspects of Title VI echo the corresponding guarantee of civil rights in employment under Title VII.[299] Establishing disparate impact under Title VI similarly proceeds in three steps. First, an agency official must establish that a facially neutral policy disproportionately harms one of the relevant protected class members—here, most likely students of color, particular origins, or religious affiliations whose observance involves headwear.[300] Once a prima facie case is established, a school must have a "substantial legitimate justification" for the challenged practice, proof of which generally involves a showing that the challenged policy was "necessary to meeting a goal that was legitimate, important, and integral to the [recipient's]

---

http://www2.ed.gov/about/offices/list/ocr/letters/colleague-201401-title-vi.pdf ("Schools also violate Federal law when they evenhandedly implement facially neutral policies and practices that, although not adopted with the intent to discriminate, nonetheless have an unjustified effect of discriminating against students on the basis of race . . . commonly referred to as 'disparate impact.'"); U.S. DEP'T OF JUST., C.R. DIV., TITLE VI LEGAL MANUAL § IX(A) (2021).

[295] U.S. DEPT. OF EDUC., OFF. FOR C.R., *supra* note 289, § 102.

[296] *Id.* § V(C)(4).

[297] *Id.* § I(C)(4); Jared P. Cole, Cong. Rsch. Serv., R45665, Civil Rights at School: Agency Enforcement of Title VI of the Civil Rights Act of 1964 17 (2019).

[298] 42 U.S.C. § 2000d-1.

[299] U.S. DEP'T OF JUST., C.R. DIV., *supra* note 294, § VII(C) ("The elements of a Title VI disparate impact claim are similar to the analysis of cases decided under Title VII."); *see also* N.Y. Urban League, Inc. v. New York, 71 F.3d 1031, 1036 (2d Cir. 1995).

[300] *See* Larry P. *ex rel.* Lucille P. v. Riles, 793 F.2d 969, 982 (9th Cir. 1984); 28 C.F.R. § 42.104(b)(2) (2022).

institutional mission."[301] A practice justified by educational necessity may still violate Title VI if there is an equally effective, less discriminatory alternative.[302]

To establish liability for disparate impact under the Title VI regulations, OCR must first find that a facially neutral practice—here, using online proctoring—has a disproportionately adverse effect on a protected group.[303] It must (1) identify the specific policy or practice at issue; (2) establish adversity/harm; (3) establish significant disparity; and (4) establish causation.[304] Most complaints of testing discrimination in education involve the substance of a test itself rather than the conditions of its administration.[305]

OCR guidance indicates that a test generally has a disproportionate adverse impact if a statistical analysis shows a significant difference in results of a protected class from the expected random distribution of test scores.[306] As noted above, the automated components of OPTs are likely to have a disproportionately negative impact on several protected classes, including students who present as female, have darker skin, wear religious headwear, or have medical conditions or disabilities.[307] But this does not mean there is sufficient evidence to establish a prima facie case of disparate treatment.

There are several obstacles to establishing statistically significant disparate impact. Like many automated systems, OPTs' algorithmic opacity obscures the statistical evidence or causality required to

---

[301] The context-specific "educational necessity" must be legitimate, important, and integral to the defendant's institutional mission. Elston v. Talladega Cnty. Bd. of Educ., 997 F.2d 1394, 1413 (11th Cir. 1993). The practice must also demonstrate a relationship to that goal. Ga. State Conf. of Branches of NAACP v. Georgia, 775 F.2d 1403, 1417–18 (11th Cir. 1985).

[302] 34 C.F.R. § 100.3(b)(2) (2022); *see* Young *ex rel.* Young v. Montgomery Cnty. Bd. of Educ., 922 F. Supp. 544, 550 (M.D. Ala. 1996); African Am. Legal Def. Fund, Inc. v. N.Y. State Dep't of Educ., 8 F. Supp. 2d 330, 338 (S.D.N.Y. 1998) (holding that plaintiff's proposed alternative formula for computing school funding, determined by enrollment numbers instead of attendance, was legally insufficient because it did not satisfy the purpose served by the prevailing formula).

[303] *Elston*, 997 F.2d at 1407.

[304] N.Y.C. Env't Just. All. v. Giuliani, 214 F.3d 65, 69 (2d. Cir. 2000).

[305] *See, e.g.*, Complaint, Smith v. Regents of the Univ. of Cal., No. RG19046222 (Cal. Super. Ct. Dec. 10, 2019); Kimberly West-Faulcon, *More Intelligent Design: Testing Measures of Merit*, 13 U. PA. J. CONST. L. 1235, 1281–85 (2011).

[306] U.S. DEP'T OF EDUC., OFF. FOR C.R., THE USE OF TESTS AS PART OF HIGH-STAKES DECISION-MAKING FOR STUDENTS: A RESOURCE GUIDE FOR EDUCATORS AND POLICY-MAKERS (2000), https://www2.ed.gov/offices/OCR/archives/pdf/TestingResource.pdf.

[307] *See supra* Section I.A.3.

establish disparate impact.[308] Trade secret protection may also prevent in-depth scrutiny of data inputs and the machine-learning model.[309] Again, OPTs' abysmal inaccuracy may preclude a finding of disparate impact—proctoring artificial intelligence may simply err across the board.[310] Even upon finding prima facie disparate impact, schools have a strong defense: They can claim that remote proctoring was an educational necessity required to protect a legitimate interest in preventing students from cheating. Further, schools can assert that they had no less discriminatory alternatives given pandemic exigencies.[311]

3. The Americans with Disabilities Act and the Rehabilitation Act of 1973

Discrimination claims based on disability face the same substantive problems as Title II complaints, along with additional procedural barriers. Title II of the ADA and Section 504 prohibit schools from discriminating against students—or other individuals—on the basis of their disabilities.[312] While Title II's reach extends only to state and local government activities, including public colleges, universities, and graduate schools, Section 504 covers all programs receiving federal financial assistance, which includes some private schools.[313] The same liability and compliance standards apply to the

---

[308] *See, e.g.*, Kim, *supra* note 285; Barocas & Selbst, *supra* note 285; Datta et al., *supra* note 285; BOGEN & RIEKE, *supra* note 285; Raub, *supra* note 285.

[309] Dallas Card, *The "Black Box" Metaphor in Machine Learning*, MEDIUM, (July 5, 2017), https://dallascard.medium.com/the-black-box-metaphor-in-machine-learning-4e57a3a1d2b0; Hous. Fed'n of Tchrs. v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168 (S.D. Tex. 2017) (holding that plaintiff teachers could establish that a school district violated their due process rights when a vendor refused to reveal elements of the database and algorithm that made termination decisions); *see* Wexler, *supra* note 193 (discussing machine learning in the context of criminal justice algorithmic risk assessments).

[310] *See supra* Section I.B.3.

[311] Tsombanidis v. W. Haven Fire Dep't, 352 F.3d 565, 575 (2d Cir. 2003).

[312] B.C. v. Mount Vernon Sch. Dist., 837 F.3d 152, 158 (2d Cir. 2016). While the ADA's reach extends only to state and local government activities, including public colleges, universities, and graduate schools, Section 504 covers all programs receiving federal financial assistance, which includes some private schools. 29 U.S.C. § 794; *see Race and National Origin Discrimination: Frequently Asked Questions*, U.S. DEP'T OF EDUC., OFF. FOR C.R., https://www2.ed.gov/about/offices/list/ocr/frontpage/faq/race-origin.html (last visited Nov. 19, 2022).

[313] 29 U.S.C. § 794.

ADA and Section 504, which are generally invoked together in disability discrimination litigation.[314]

Eligible students who are denied their allotted time to take a test or disciplined due to too many false flags could claim that the school denied them appropriate accommodations under the Individuals with Disabilities Education Act (IDEA). Successful IDEA complaints could rectify an individual's circumstances by requiring schools to provide the requisite accommodation or compensatory damages.[315] However, students would not be able to proceed to federal court until they exhaust a state's IDEA administrative process, which is extraordinarily difficult to do in practice.[316]

Unlike Title VI, aggrieved students may file ADA or Section 504 discrimination claims for injunctive and monetary relief in federal court.[317] To do so, however, the "gravamen" of a student's complaint must allege disability-based discrimination rather than denial of an education benefit, such as the right to a free, appropriate public education guaranteed by IDEA.[318]

Students must allege discriminatory, not educational harms to bring claims in federal court.[319] In *Fry v. Napoleon Community Schools*, the Supreme Court noted that the substance of a claim is likely to be discrimination if the plaintiff could bring essentially the same claim if the alleged conduct had occurred at a public facility that was not a school or if an adult could bring essentially the same grievance.[320] It would be challenging to characterize the substance of a complaint based on online proctoring as disability-related discrimination, since

---

[314] D.A. v. Hous. Indep. Sch. Dist., 629 F.3d 450, 453 (5th Cir. 2010); Pace v. Bogalusa City Sch. Bd., 403 F.3d 272, 287 (5th Cir. 2005) (en banc); Hainze v. Richards, 207 F.3d 795, 799 (5th Cir. 2000).

[315] *See, e.g.*, G.L. v. Ligonier Valley Sch. Dist. Auth., 802 F.3d 601 (3rd Cir. 2015) (holding that compensatory education may be an IDEA remedy).

[316] Fry v. Napoleon Cmty. Schs., 580 U.S. 154 (2017).

[317] Alexander v. Choate, 469 U.S. 287, 299 (1985) (stating "§ 504 reaches at least some conduct that has an unjustifiable disparate impact upon the handicapped"); *Fry*, 580 U.S. 154 (holding that parents need not exhaust remedies and bring a special education hearing before bringing a lawsuit in federal court for a school discrimination case). To bring a claim in federal court, the "gravamen" of the students' complaint must allege discrimination rather than denial of an education benefit. *Id.*

[317] *Id.* (establishing a prime facie case of disparate impact requires: "(1) the occurrence of certain outwardly neutral practices, and (2) a significantly adverse or disproportionate impact on persons of a particular type produced by the defendant's facially neutral acts or practices, and (3) a causal connection between the facially neutral policy and the alleged discriminatory effect").

[318] *Fry*, 580 U.S. 154 (2017).

[319] *Id.*

[320] *Id.*

the most salient harm is its impact on students' performance or students being subject to school discipline. Students who pass these procedural hurdles would have the same problems of proof as with the Title VI actions above. Accordingly, antidiscrimination claims against OPTs have only a remote possibility of success.

III. EXTRA-LEGAL LEVERS: TECHNICAL, INSTITUTIONAL, AND PEDAGOGICAL REFORM

As the prior section shows, students cannot rely on existing legal mechanisms to address the pandemic use of proctoring technologies or ensure that they will not be subject to similarly problematic technologies in the future. Pursuing algorithmic accountability through FERPA is better than nothing, but it burdens both students and schools. Proactive action by regulators is uncertain at best. Accordingly, this article suggests extra-legal approaches that do not require legal or political action.[321]

Under these circumstances, the most ethical response to flawed proctoring technologies would be a moratorium on their use until sufficient evidence supports their accuracy, efficacy, and impact on equity. This would also give schools time to create better systems to train educators and supervise automated decision-making. Until then, companies should not offer and schools should not use unproven services like automated cheating detection. Both companies and schools should reject facial characterization and behavioral profiling technologies based on pseudoscience. Doing so will enable them to eliminate, or at least reduce, invasive surveillance.

However, a moratorium is preferable to a ban. As more and more nontraditional students pursue credentials, they must have a way to do so from a distance. Selective use of evidence-based, minimally invasive platforms with responsible school administration could expand access to opportunity by allowing completely remote students to earn recognized academic credentials.[322]

---

[321] For additional suggestions, *see also* David Luinstra, *The Use of Eproctoring Software at Post-Secondary Institutions: A Balanced Approach*, *in* 2 ETHICAL USE OF TECH. IN DIGITAL LEARNING ENVIRONMENTS: GRADUATE STUDENT PERSPECTIVES 20 (Barbara Brown et al., eds., 2021).

[322] Coghlan et al., *supra* note 12, at 1952 ("Companies claim that well-designed AI can also mitigate human bias and error . . . .").

A. Technical Reform

Companies need to take responsibility for the accuracy and impact of their services without hiding behind the claim that they offer mere decision support. Vendors must not only ensure that students are not unfairly punished but provide enough information and opportunities for appeal to reassure test-takers that they have accounted for inevitable technical errors. They must also bolster student privacy by minimizing data collection, redisclosure, and retention, especially audiovisual feeds capturing students in their home environments. They should solicit input from school customers and student users about their needs, concerns, and obstacles. The following suggestions offer a minimum baseline /place to start.

1. Improve—and Prove—Accuracy and Efficacy Across Diverse Populations and Environments

Companies that continue to use automated systems must train and test their systems to ensure baseline accuracy across diverse populations and testing environments. They must vet their software thoroughly and thoughtfully, ideally by collecting empirical evidence to support reliability, efficacy, accuracy, and fairness claims. Vendors that continue to offer automated proctoring must subject their systems to rigorous, third-party scrutiny to assess their accuracy and potential bias. These could include data protection impact assessments, which are crucial components of Europe's GDPR.[323] Algorithmic impact statements could also help address algorithmic bias and ensure greater accountability. Modeled on environmental impact statements required under federal law, these are more formal analyses of the potential impact of automated decision systems on fairness, justice, bias, and other concerns across affected communities.[324]

Having conducted these inquiries, vendors should acknowledge the limitations of algorithmic analysis and instruct educators about signs that suggest an algorithmic determination requires human review.

---

[323] DILLON REISMAN ET AL., AI NOW INST., ALGORITHMIC IMPACT ASSESSMENTS: A PRACTICAL FRAMEWORK FOR PUBLIC AGENCY ACCOUNTABILITY (2018), https://ainowinstitute.org/publication/algorithmic-impact-assessments-report-2; Margot E. Kaminski & Gianclaudio Malgieri, *Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR*, *in* PROCEEDINGS OF THE CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 68 (2020).

[324] DILLON REISMAN ET AL., AI NOW INST., ALGORITHMIC IMPACT ASSESSMENTS: A PRACTICAL FRAMEWORK FOR PUBLIC AGENCY ACCOUNTABILITY (2018), https://ainowinstitute.org/publication/algorithmic-impact-assessments-report-2.

It is irresponsible to rely on educators to make up for OPTs' technical flaws, because it ignores the fact that educators can only review a small proportion of OPT software's flags and reports. Vendors who do use facial analysis should update their systems to meet state-of-the-art standards for accuracy and bias.

2. Reject Fundamentally Flawed Technologies

Improving accuracy is not enough for services based on questionable scientific foundations, like the ability to create a profile of "normal" test-taking activity and the assumption that deviation from that baseline indicates academic misconduct. OPTs should stop using unproven cheating detection analytics that rely on faulty assumptions, such as the existence of a "normal" pattern of test-taker behavior. ProctorU set an excellent example in response to criticism by reassessing its technologies and assumptions about how schools would implement them.[325] The company acknowledged that its automated proctoring system generated too many false positives, often flagging students for innocuous movements or typical home environments. When the vendor discovered that its customers were not, in fact, reviewing machine-generated results, it stopped offering completely automated proctoring services.[326] Other companies should follow suit and have a human-in-loop review of automated inferences. Those who don't must devote considerable resources to ensure that automated systems operate accurately across a variety of populations and testing environments, including home settings, and must institute sufficient internal human review to account for an overabundance of false flags.

OPTs should also account for inevitable errors by creating systems that allow students to begin and complete tests and then address problems through internal post-exam review. ExamSoft, for example, permits students to take assessments even if they have authentication problems or are flagged for problematic behavior mid-exam.[327] Vendors must implement sufficient internal oversight to account for both human and automated errors—without making this

---

[325] Jaschik, *supra* note 144.
[326] *Id.*
[327] *ExamID: Exam Integrity and Authentication Streamlined to Make Exam Day More Secure*, EXAMSOFT, https://f.hubspotusercontent40.net/hubfs/2956392/Collateral/One_Pagers/ExamSoft_ExamID.pdf.

oversight an expensive addition to core services. These reforms save students precious time during exams and allow them to proceed with less anxiety about verification problems and false flags.

3. Adopt Proactive Privacy and Security Standards

Finally, OPTs need to adopt basic privacy protections. Vendors who claim to protect students' privacy may do little more than implement commonplace security precautions that protect against bad actors, like encryption.[328] Companies need to embrace data minimization, reducing the types of data they collect about students and imposing short retention limits. They must have technical systems that prevent instructors and administrators from downloading and sharing audiovisual recordings. Professional human proctors should be trained and required to uphold privacy best practices.[329]

ProctorU took steps in this direction by adopting a "Student Bill of Rights for Remote and Digital Work."[330] Among other rights, the document says that students can expect to have their questions answered, be presumed to be honest and accurate, and be served by entities compliant with laws and regulations related to student privacy and student data. They also have the right to review personal data and to understand why specific and limited data are collected and whether such data is shared.[331]

---

[328] *Automated or Live Online Proctoring*, *supra* note 53. ("Test-taker privacy first 1. Limited access to test-taker data Encrypted test-taker exam recordings can be decrypted by institution-approved representatives. 2. Test-taker data is kept safe Test-taker exam recordings are stored in institution-approved data centers.").

[329] For additional examples, *see* ASS'N FOR COMPUTING MACH., U.S. TECH. POL'Y COMM., STATEMENT ON PRINCIPLES FOR THE DEVELOPMENT AND DEPLOYMENT OF EQUITABLE, PRIVATE, AND SECURE REMOTE TEST ADMINISTRATION SYSTEMS (2021), https://www.acm.org/binaries/content/assets/public-policy/ustpc-statement-remote-test-admin-systems.pdf; INT'L PRIVACY SUBCOMM. OF THE ATP SECURITY COMM., *supra* note 45.

[330] ProctorU's "Bill of Rights" states that students have a right to (1) prompt answers to questions about remote assessment; (2) a presumption of honesty; (3) compliance with privacy laws; (4) established policies regarding ensuring the integrity of remote or digital work and the right to access and review these policies; (5) establishing policies and the right to access and review policies to ensure that they are not unfairly disadvantaged by other students' misconduct; (6) understand what data may be collection, how it is stored, and whether it is disseminated and to require it not be sold or transferred; and (7) specific and limited data collection. STUDENT BILL OF RIGHTS, https://studenttestingrights.org/ (last visited Nov. 19, 2022).

[331] *Id.*

B. Institutional Reform

Schools' lack of oversight was understandable in the first days of the pandemic. It is now inexcusable. Educators must accept responsibility for testing technologies' flaws and fundamental limitations. This includes providing accessible processes and FERPA-mandated access so students can challenge vendors' inferences. Schools should not use unproven software with inadequate oversight. Further, they should require students to use proctoring technologies only in limited circumstances when there is no other way to provide access to opportunity. Schools should also take measures to ensure that their implementation of OPTs is fair and accountable with sufficient teacher training, clear and transparent communication to students, and standardized thresholds for sufficient levels of accuracy to ensure due process. They must put both ex ante and ex post protections in place by choosing only evidence-backed services bolstered by vendor-provided human oversight, train teachers, provide accessible processes and FERPA-mandated access so that students can challenge vendors' inferences, and communicate and consult with students.[332] Schools must also consider and minimize the social, emotional, and psychological harms wrought by uncertain proctoring technology and its intrusive surveillance. The suggestions below require schools to reconsider aspects of their rushed adoption of OPTs and implement them in a more thoughtful, accountable, and transparent fashion.

1. Choose Proctoring Vendors and Services Carefully, If At All

Schools must exercise discretion when choosing OPT vendors and services. At a minimum, they should include a legally enforceable confidentiality clause regarding how the proctor handles test-takers' personal information to ensure that it is not disclosed to unauthorized persons. Schools should require vendors to train their employees and

---

[332] *See* Coghlan et al., *supra* note 12, at 1602.

proctors about data privacy.[333] Most significantly in the context of OPTs, contracts should specify that vendors will give students sufficient access to personally identifiable student information to satisfy FERPA's requirements and provide teachers, administrators, or students with enough data to support an independent evaluation of OPTs' algorithmic assessments and inferences.

Schools can pressure vendors to improve their products by only adopting vetted and empirically supported systems. Schools must conduct their own reviews of education technologies that do more than merely ensure that vendors' data practices and terms of service do not include blatant FERPA violations. These audits should include inquiring about the procedures in place to cope with technical problems. And, importantly, they should involve careful scrutiny of companies' promises about emerging technologies.

Schools can also choose not to use problematic components of OPTs even if vendors do not make the aforementioned technical reforms.[334] One study, for example, suggests that lockdown services are sufficient to prevent cheating without the need for facial analysis or audiovisual monitoring.[335] Schools that do use proctoring technologies should only do so if evidence supports that they are, in fact, necessary and effective in detecting and deterring misconduct. They cannot rely on teachers to take on the burden of reviewing completely automated proctoring but must instead purchase services that include human review.

2. Provide Training and Adequate Oversight

Schools must also acknowledge that technical improvements will not eliminate all OPT errors. They need to better train the educators who will be using the software, not only on the technology's functions but also on its problematic elements. Educators must be able to

---

[333] Int'l Privacy Subcomm., Ass'n of Test Publishers' Sec. Comm., *Privacy Considerations in Online/Remote Proctoring*, 9 PRIVACY IN PRACTICE BULLETIN 1, 7 n.5 (2020), https://www.testpublishers.org/assets/privacy%20in%20practice%20bulletin%209_%20remote%20proctoring_v3_04072020.pdf ("Controllers, processors, and sub-processors need to keep a record of all personnel trained in data privacy, including the dates on which they were trained. In the future, test proctors may be qualified through an annual certification exam that includes data privacy elements.").

[334] University of Wisconsin–Madison, for example, turned off an Honorlock feature that disabled exams when students look away or use low lighting. *See* Meyerhofer, *supra* note 26.

[335] Pleasants et al., *supra* note 132.

recognize results that indicate a potential problem. Administrators should develop formal protocols for proctoring technology oversight—for example, specifying under what circumstances teachers should review algorithmic determinations. They also need to develop ways to evaluate OPTs' accuracy, efficacy, and impact on students on an ongoing basis. Schools also need to create an accessible appeal system for students to contest adverse outcomes—and comply with FERPA's requirements to give students the ability to defend themselves.

3. Student-Centered Communication, Consent, and Contestation Policies

Schools and vendors must be transparent about their data collection and analysis, privacy practices, and institutional procedures. Commentators often point to proctoring technologies as being anxiety-inducing. But as much of the blame rests on schools that should have anticipated software errors and student stress. Educators can drastically reduce student anxiety through simple communication. Students need to know that certain necessary behaviors—such as looking away from a monitor or taking a bathroom break—will not lead to cheating allegations. They further deserve reassurance that schools would resolve authentication problems and false flags through adequate oversight and an appeal process.

C. Pedagogical Reform

Finally, instructors should change their pedagogy and adopt more sophisticated and meaningful assessment protocols that do not depend on limiting students' access to the internet. The changes above would significantly improve students' experience of online proctored tests and support more equitable and accountable outcomes. However, tweaking user interfaces, fleshing out privacy policies, and training teachers cannot address the fundamental problems posed by proctoring technologies: they rely on unfair, unproven, and intrusive technology.

The best solutions would remove the need for proctoring in the first place. Whenever possible, educators should administer assessments that do not require constant monitoring to ensure academic integrity by, for example, assigning projects instead of examinations or designing open-book tests. Doing so is challenging, but

possible, as demonstrated by schools who discouraged[336] or prohibited[337] teachers from using proctoring technologies during the pandemic. Alternative assessments not only avoid the OPT problems noted above but are also superior from a pedagogical standpoint.[338] Assignments requiring students to apply what they have learned are more accurate and relevant ways to assess student mastery than student recall.[339] Unsurprisingly, the schools that were able to reject proctoring technologies are more elite[340]—those that do not have to worry as much about undermining their reputation for academic integrity. However, all schools can, and should, at least reduce reliance on the kind of tests that require proctoring.[341] As much as possible, they should limit the use of OPTs to circumstances where testing memorization is essential, such as when healthcare students take anatomy tests and when students have no other way to earn verified credentials, such as completely remote certification programs. Educators and schools should also try to cultivate a less transactional view of education, which researchers show reduces student cheating.[342]

CONCLUSION

Today's proctoring technologies create inexcusable flaws that disproportionately harm members of marginalized communities. However, students and advocates have little legal leverage to prompt change. At best, they can employ FERPA's right of access to promote algorithmic fairness and obtain due process.

---

[336] *See, e.g.*, *Remote Exams and Assessments: Tips for Exams and Alternative Assessments*, RUTGERS SCH. OF ARTS & SCIS., https://sasoue.rutgers.edu/teaching-learning-guides/remote-exams-assessment (last visited Nov. 19, 2022) (providing examples for student evaluation such as more frequent Canvas-based quizzes, open-book exams, portfolios, or group projects in place of online-proctored exams).
[337] *Protect Student Privacy: Ban Eproctoring*, *supra* note 25.
[338] *See, e.g.*, JAMES LANG, CHEATING LESSONS (2013); Elaine H. J. Yew & Karen Goh, *Problem-Based Learning: An Overview of Its Process and Impact on Learning*, 2 HEALTH PROS. EDUC. 75 (2016).
[339] *See supra* Section III.C.
[340] Schwartz, *supra* note 38.
[341] *See supra* Section III.C.
[342] A meta-analysis of seventy-nine papers studying the motivations behind academic honesty and academic dishonesty found that students who perceive assessment structure as based on developing mastery of particular skills, and who are convinced that the course is useful, are less likely to cheat. Megan R. Krou et al., *Achievement Motivation and Academic Dishonesty: A Meta-Analytic Investigation,* 33 EDUC. PSYCH. REV. 427 (2021); Jarret M. Dyer et al., *Academic Dishonesty and Testing: How Student Beliefs and Test Settings Impact Decisions to Cheat*, 4 J. NAT'L COLL. TESTING ASS'N 1 (2020).

At this stage of the "techlash," the paucity of student privacy protection should not be surprising. It is just another instance of innovation outpacing governance: a fundamental failure to protect against, redress, regulate, or even recognize the flaws of today's education technology.

Online proctoring may become less common as the pandemic wanes, but its example shows that students need protection against contemporary education privacy harms. But OTPs are just one of many examples of algorithmically-driven and surveillant education technologies—many of which are much more difficult to oversee or eschew. Protective measures must be put in place before schools adopt emerging technologies that may become too promising to reject, too integral to discontinue, and too invisible to stoke public outrage. This warning isn't a false flag.