SNOOPING WHERE WE SLEEP

The Invasiveness and Bias of Remote Proctoring Services

ALBERT FOX CAHN, ESQ.
CAROLINE MAGEE
DR. ELENI MANIS, PHD.
NAZ AKYOL

NOVEMBER 11, 2020

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

Executive Summary

Across the US, K-12 schools and universities have shifted to remote instruction to contain the spread of COVID-19. In doing so, an increasing number are using a dystopian set of surveillance tools to discourage cheating, including facial recognition to identify test-takers, video monitoring to flag supposedly suspicious behavior, and remote access to students' computers to control their activity during exams. The need for these tools is not clear: evidence suggests that students cheat less on online exams than in traditional classroom settings.[1] Moreover, academic surveillance tools' effectiveness at discouraging academic dishonesty is simply unknown. But while the need for and effectiveness of academic surveillance tools is not established, the dangers of such tools are. Academic surveillance tools are unfair, disadvantaging some groups of students relative to their peers: automatic flagging of suspicious behaviors penalizes students with disabilities, stigmatizing a range of normal behaviors. Facial recognition performs more poorly on dark-skinned, female, and older students, generating an unfair obstacle to identity verification, the first step in taking an online test. Academic surveillance tools require students to meet significant technological requirements, unfairly penalizing low-income students. In addition to these equity concerns, academic surveillance tools generate a data trail of suspicious behavior, justifying the tools' continued use and routinely placing students under a cloud of suspicion. These tools normalize spying on students, allowing unseen proctors to closely surveil students during exams. In their disrespect for student privacy, they pose a significant risk to students' data security. For these reasons, S.T.O.P. recommends that educational institutions stop using online proctoring services. If schools insist on adopting such tools despite their known deficiencies, the simplest, least invasive versions should be chosen, and these tools should be audited for effectiveness, bias, and adequate protection of student data.

Introduction

As COVID-19 confined millions to their homes, remote learning quickly became a fixture of daily life. What began with three states closing schools in mid-March[1] turned into a nationwide trend by the end of that month, with all fifty states ordering at least a partial closure of in-person education.[2] Many private colleges and universities followed suit, with more than 1,100 institutions

[1] *NJ Schools to Shut Down Wednesday; See Tri-State Closures Here*, NBC N.Y., https://www.nbcnewyork.com/news/local/coronavirus-closures-here-are-the-schools-closed/2317622/ (last visited: July 25, 2020)

[2] *Map: Coronavirus and School Closures*, EDUCATION WEEK, https://www.edweek.org/ew/section/multimedia/map-coronavirus-and-school-closures.html (last visited: Aug. 3, 2020).

shuttering campus.[3] Today, COVID-19 has moved more than a million post-secondary students to online classes,[4] and more than 8 million K-12 students have been impacted by school closures.[5]

And remote learning may be here to stay. Many K-12 public schools,[6] colleges, and universities[7] moved to entirely remote learning for the fall 2020 semester,[8] and some that attempted to reopen quickly abandoned the effort.[9] Given the increasing number of COVID-19 cases in many states,[10] more institutions will likely continue mixed remote and in-person instruction or move entirely to remote learning in coming months.[11]

With this major and likely long-lasting shift to remote learning in both K-12 and higher education, it is important to evaluate the implications of the various tools used by institutions to realize it. One of the most significant hurdles to remote education is evaluating student performance through online exams and assignments. To promote academic honesty and to detect cheating, educational institutions have turned to academic surveillance systems consisting of remote live proctors aided by anti-cheating software. Increasingly, these same systems are being used by

[3] Abigail Hess, *How Coronavirus Dramatically Changed College for Over 14 Million Students*, CNBC Make It (Mar. 26, 2020) https://www.cnbc.com/2020/03/26/how-coronavirus-changed-college-for-over-14-million-students.html.

[4] *See:* Brianna McGurran, *COVID-19 and College, Here's What the Fall Will Look Like*, Forbes (Aug 19. 2020), https://www.forbes.com/sites/advisor/2020/08/19/covid-19-and-college-heres-what-the-fall-will-look-like/#2e06de153ec9; *Columbia and Barnard Announce Entirely Online Fall 2020*, Bwog (Aug. 14, 2020), https://bwog.com/2020/08/columbia-and-barnard-announce-entirely-online-fall-2020/;

[5] *School Distrcits' Reopening Plans, A Snapshot*, Education Week (Sept. 22, 2020), https://www.edweek.org/ew/section/multimedia/school-districts-reopening-plans-a-snapshot.html; *see also*: Lara Fishbane, Adie Tomer, *As classes move online during COVID-19, what are disconnected students to do?*, Brookings Inst. (Mar. 20, 2020) https://www.brookings.edu/blog/the-avenue/2020/03/20/as-classes-move-online-during-covid-19-what-are-disconnected-students-to-do/.

[6] Perry Stein, *As Public Schools Go All Virtual In Fall, Parents Eye Private Schools That Say They Will Open Their Campuses*, Wash. Post (July 26, 2020) https://www.washingtonpost.com/local/education/as-public-schools-go-all-virtual-in-fall-parents-eye-private-schools-that-say-they-will-open-their-campuses/2020/07/26/1e446ab0-cc5b-11ea-b0e3-d55bda07d66a_story.html.

[7] Joey Hadden, *What the top colleges and universities in the US have said about their plans to reopen in fall 2020, from postponing the semester to offering more remote coursework*, Business Insider (July 28, 2020) https://www.businessinsider.com/how-major-us-colleges-plan-reopen-for-fall-2020-semester-2020-5#princeton-university-17; https://www.cnn.com/2020/07/13/us/school-reopening-plans-major-cities/index.html.

[8] Erica Schwiegershausen, *When Will Schools Reopen?*, Cut (July 29, 2020) https://www.thecut.com/2020/07/will-schools-open-in-the-fall-reopening-statuses-explained.html.

[9] *See*: Press Release, SUNY, Chancellor Malatras Directs SUNY Oneonta to Transition All Students to 100% Remote Learning Off Campus for Fall Semester Following Nearly 400 COVID-19 Cases (Sept. 3, 2020), https://www.suny.edu/suny-news/press-releases/09-2020/9-3-20/oneonta-transitions-remote-learning.html; *SUNY Cortland Passes 100-Case Threshold; Will Move To Remote Learning*, WBNG (Oct. 6, 2020, 2:13 AM), https://wbng.com/2020/10/06/suny-cortland-passes-100-case-threshold-will-move-to-remote-learning/; *Stanly County School Moving to Virtual Learning After Multiple Positive COVID Cases Confirmed Among Staff*, WCNC (Oct. 6, 2020, 11:24 PM), https://www.wcnc.com/article/news/education/north-stanly-high-school-going-virtual-for-two-weeks/275-e21a4f6c-f6ac-4c1f-81a6-3976ddc21b51.

[10] *Coronavirus in the US: Latest Map and Case Count*, N.Y. Times, https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html (last visited: Aug. 3, 2020).

[11] *See*: *UC Berkley To Begin Spring Semester With Fully Remote Learning* (Sept. 29, 2020, 4:42 PM), https://sanfrancisco.cbslocal.com/2020/09/29/uc-berkeley-to-begin-spring-semester-with-fully-remote-learning/; Michael Alachnowicz, *Virginia's Community Colleges To Continue Remote Learning For Spring Semester*, WDBJ (Sept. 21, 2020, 5:25 PM), https://www.wdbj7.com/2020/09/21/virginias-community-colleges-to-continue-remote-learning-for-spring-semester/.

professional accreditation organizations, such as state bar examiners and the United States Medical Licensing Examination.[12]

Academic surveillance systems use a myriad of invasive methods, including eye-tracking, facial recognition, video and audio surveillance, and remote access to students' computers. These surveillance tools are unfair, penalizing vulnerable groups of students for their disabilities and for being non-white, female, older, or being low-income. Academic surveillance tools are exquisitely suspicious, flagging a wide range of innocent behaviors for investigation, with a predictably negative impact on student welfare. In their blatant disregard for students' privacy, they generate and retain sensitive student data and pose an additional security risk to students' computer files.

For these reasons, academic surveillance tools should be avoided. Schools have been too quick to replace pedagogical solutions, such as honor codes, that have been in effect for centuries and have proven success.[13] If schools must use surveillance tools, only the least invasive remote education technologies should be considered, and even then with caution and significant attention to accountability and independent auditing.

Part I: The Proliferation of Academic Surveillance Technology

Educational and licensing institutions are turning to academic surveillance tools in unprecedented numbers, citing anxieties about academic integrity within the framework of online learning. Under the banner of "online proctoring," schools are engaging in extensive student surveillance to supervise examinations and evaluations remotely.[14] Typically, a student is monitored while completing an assignment or exam using a combination of tools including the student's webcam, microphone, and screen. Access is granted to these tools on the student's device through third-party platforms.

The move to online surveillance of students matches recent growth in online learning. Even before the COVID-19 pandemic, nearly 7 million students in the US were enrolled in online college education.[15] As a result of the COVID-19 pandemic, this number has skyrocketed: in June 2020, 97% of college students reported switching to online instruction.[16] The market for online higher education could reach $74 billion globally by 2025, up from $36 billion in 2019.[17]

[12] Emma Goldberg, *Bar and Medical Exam Delays Keep Graduates in Limbo*, N.Y. TIMES (Sep 4, 2020), https://www.nytimes.com/2020/09/04/us/bar-exam-coronavirus.html.

[13] *See*: David Callahan, *Why Honor Codes Reduce Student Cheating*, HUFFPOST (May 25, 2011), https://www.huffpost.com/entry/why-honor-codes-reduce-st_b_795898?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABBac9JS4l8q-PhpF_0x_OM7WefxZBAWJtRVSXvcjA6_woDRqHn7Dl7-v5WMpiOIhNuLHuwyyN6rEdlw2bkZlcKeQQ67HWi1wh2imAiQFgZzwvdsslQF_vdB-1I0vlGQ2TkP743CtUdtMGWWxh3seTXHc9oNVetGGZCD3NmY45bg.

[14] Anushka Patil and 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.

[15] *Distance Learning*, NAT'L CTR. EDUC. STATISTICS, https://nces.ed.gov/fastfacts/display.asp?id=80 (last visited: Aug. 3, 2020).

[16] *Online Education Statistics*, EDUCATIONDATA.ORG, https://educationdata.org/online-education-statistics/ (last visited: Aug. 3, 2020).

[17] $74B Online Degree Market in 2025, Up From $36B in 2019, HOLONIQ (May 1, 2020). https://www.holoniq.com/notes/74b-online-degree-market-in-2025-up-from-36b-in-2019/; see also: Natasha Singer,

With an unprecedented number of students enrolled in online education, American higher education institutions have rushed to deploy third-party student surveillance platforms and software to prevent allegedly dishonest behavior.[18] An April 2020 poll by Educause, an education technology organization, found that 54% of the higher education institutions polled were using "online proctoring" services, and an additional 23% were considering or planning on using them in the near future, even though over half of the institutions polled said they were concerned about cost and student privacy.[19] One representative company, Examity, reported a 35% increase in growth from one quarter to the next during the COVID-19 crisis. Other popular platforms include PSI Services, Mercer|Mettl, ProctorU, Proctorio, Examsoft, Examity, and Verificient.[20]

While there is clear evidence that academic surveillance is dangerous, there is little evidence that it is effective at preventing cheating or that online evaluations require extraordinary anti-cheating measures. Prior to the COVID-related rush to remote instruction, educators also feared that students would cheat more often in online courses. These suspicions were demonstrated to be unfounded: students cheat more in in-person classes than in online ones.[21]

That said, the switch to remote learning may warrant alternative student assessment techniques.[22] Many colleges[23] and K-12 schools moved to pass/fail grading as part of their transition to online education in the spring.[24] These changes acknowledge the painful reality that it is impossible to conduct fair, high-stakes tests when some students are able to take tests in sprawling home offices, and others take tests while crammed into a closet, a restroom, or outside a Taco Bell.[25]

Part II: Academic Surveillance Tools

Academic surveillance tools broadly fit into three categories. First, spyware monitors a student's computer, identifying any other applications in use. Spyware can include a log of every

Online Test-Takers Feel Anti-Cheating Software's Uneasy Glare, N.Y. Times (Apr. 5, 2015), https://www.nytimes.com/2015/04/06/technology/online-test-takers-feel-anti-cheating-softwares-uneasy-glare.html.

[18] Colleen Flaherty, *Big Proctor*, Inside Higher Ed (May 11, 2020) https://www.insidehighered.com/news/2020/05/11/online-proctoring-surging-during-covid-19.

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

[20] Nilam Oswal, *14 Best Online Exam Proctoring Software to Look Up*, Software Suggest (May 19, 2020) https://www.softwaresuggest.com/blog/best-online-exam-proctoring-software/; Patil and Bromwich, *supra.*

[21] *See* Watson, G., Sottile, J., *Cheating in the Digital Age: Do Students Cheat More in Online Courses?*, 13 Online J. of Distance Learning Admin. 1 (2010) (finding that students actually cheated more in live classes than in online ones). *See also* Beck, V., *Testing a model to predict online cheating—Much ado about nothing*, 15 Active Learning in Higher Educ. 65 (2014) (using a method other than student self-reporting and finding that students are no more likely to cheat in online setting as they are in live settings).

[22] Alec Snyder, *N.Y.C. schools change traditional grading system in response to Covid-19*, CNN (Apr. 28, 2020) https://www.cnn.com/2020/04/28/us/new-york-city-grading-system-change-covid-19/index.html.

[23] Mary Retta, *How Colleges Are Grading Students During Coronavirus*, NPR (Apr. 10, 2020) https://www.npr.org/2020/04/10/830622398/how-colleges-are-grading-students-during-coronavirus.

[24] Pam Chickering Wilson, *Jefferson schools move to pass/fail during COVID-19 closure*, Daily Jefferson Cty. Union (Apr. 14, 2020) https://www.dailyunion.com/news/covid-19/jefferson-schools-move-to-pass-fail-during-covid-19-closure/article_b2bc2917-7a32-5ae5-aec0-830bb5de3e7d.html.

[25] Alisha Ebrahamji, *School Sends California Family a Hotspot After Students Went to Taco Bell to Use Their Free Wi-Fi*, CNN (Aug. 31, 2020, 10:28 PM) https://www.cnn.com/2020/08/31/us/taco-bell-california-students-wifi-trnd/index.html.

keystroke and mouse click a student makes, as well as looking at a student's existing software. Second, schools can use a proprietary "lockdown browser" that provides heavily restricted internet access. Third, educators can use a student's own webcam to conduct persistent video and audio surveillance. These recordings capture the most intimate confines of a student's home, and are reviewed by computer vision software and live proctors for signs of cheating.

The surveillance process begins at the outset of an online exam, when academic surveillance tools use a combination of video footage and facial recognition technology to verify students' identities. Students are often asked to use a government-issued identification card and may be asked to place their ID card in plain view of their webcam. Taking ID verification a step further, ProctorU, one commonly used academic surveillance service provider, uses facial recognition technology to scan the student's face from webcam footage and to match it to the image on the ID card presented, continuously conducting scans throughout the exam and repeating the matching process to reverify the student's identity.[26] Proctortrack, another commonly used surveillance program, requires students to bring their face and knuckles up close to the camera so that the program can scan students' features and verify their identities before a test.[27]

Student identity is also sometimes verified using typing tests, where a student is asked to type 140 words at the beginning of the semester and then again just before a test so that the surveillance program can match the speed and rhythm of the keystrokes between the two instances, confirming the student's identity.[28]

At the start of an exam, students may also be asked by the surveillance tool or a live proctor on the other side of their webcam to scan their surroundings and the top of their desk or workspace using their webcam. This kind of scan also might occur after artificial intelligence "flags" a student as a potential cheater for actions such as looking down, the student moving her face out of frame, or a loud noise off-camera, and then a live proctor may review that footage.[29]

After ID verification and an initial scan of a student's surroundings, restrictive software can be deployed to access a student's computer and disable functionalities such as being able to open documents or a browser window. This is done by giving the academic spyware full administrative access to the student's system, able to access every file and program on their computer.[30] Full access can be used for everything from monitoring whether a student copies and pastes information from an outside document to looking at a student's saved photos and videos. The software may then store this information for later review by school administrators or professors or use it to send alerts to

[26] 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/; Lawrence Abrams, *ProctorU Confirms Data Breach After Database Leaked Online*, BLEEPINGCOMPUTER (Aug. 9, 2020, 2:02 PM), https://www.bleepingcomputer.com/news/security/proctoru-confirms-data-breach-after-database-leaked-online/ (ProctorU has already professed to one breach in which 440,000 user profiles were leaked, including names, addresses, phone numbers, affiliated organizaitons, and more).

[27] Singer, *supra*.

[28] *7 Things You Should Know About Remote Proctoring*, EDUCAUSE LEARNING INITIATIVE, https://www.csustan.edu/sites/default/files/groups/Office%20of%20Academic%20Technology/examproctoring.pdf (last visited: Aug. 3, 2020).

[29] Jason Kelley and Lindsay Oliver, *Proctoring Apps Subject Students to Unnecessary Surveillance*, EFF (Aug. 20, 2020) https://www.eff.org/deeplinks/2020/08/proctoring-apps-subject-students-unnecessary-surveillance.

[30] *How it works*, PROCTORU, https://www.proctoru.com/proctoru-live-resource-center#how (last visited: Aug. 4, 2020).

remote proctors watching the student taking the exam. Most companies do not publish promising data retention guidelines, which means they may keep students' deeply intimate information indefinitely.[31]

Once the exam begins, academic surveillance technology typically uses a student's webcam and microphone to listen to, watch, and record the student's every move. This continuous video and audio monitoring is either analyzed by artificial intelligence or by a remote live proctor. Automated systems appear to be exquisitely sensitive to and suspicious of student behavior: for example, ProctorU's AI system flags students with a potential "violation" if they look off screen for four straight seconds or more than two times in a single minute.[32]

Some services rely more heavily on AI to determine flags on a student's behavior; others include a human proctor who observes "every second" of the exam, coupled with AI.[33] A remote live proctor might similarly monitor a student for behavior that the provider has flagged as "suspicious." If a student is suspected of cheating, a more aggressive specialist called an "interventionist" may be contacted.[34] A proctor or interventionist may, at any point during an exam, demand a student to aim their webcam at a certain area or follow other instructions to allow for further surveillance. Students may risk academic penalties if they refuse these demands, however, distracting or intrusive.

Attention-tracking software of the kind used by ProctorU, Proctortrack, and other academic surveillance products precedes its use in remote exam-taking. Indeed, it has been used in other contexts, where it has sparked outrage. Zoom, a videoconferencing platform, contained secret data mining[35] and attention-tracking[36] features that let the meeting host know who was paying attention during the call by alerting them if participants clicked away from the Zoom screen for more than 30 seconds. This attention tracking feature was removed at the beginning of April 2020 due the widespread outrage it sparked among users and privacy advocates.[37]

Part III: Unfair Academic Surveillance Technology—How Spyware Worsens Inequality

Academic surveillance is intended to ensure the integrity and fairness of online exams: that is, to ensure that students' grades reflect their own work and their academic skills and preparedness.

[31] See: ExamSoft, ExamSoft Privacy Policy, https://examsoft.com/privacy-policy (as long as they have an "ongoing business need" and when that is over, "either delete or anonymize/de-identify it or, if this is not possible (for example, because the data has been stored in backup archives), then ExamSoft will securely store the personal data and isolate it from any further processing until deletion is possible."); ProctorU, ProctorU Privacy Policy, https://www.proctoru.com/privacy-policy ("as long as necessary").

[32] Harwell, *supra*.

[33] *Id.*

[34] *Id.*

[35] Aaron Krolik & Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, N.Y. TIMES (Apr. 2, 2020) https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html.

[36] Jenna Amatulli, *Zoom Can Track Who's Not Paying Attention In Your Video Call. Here's How.*, HUFFINGTON POST (Mar. 25, 2020) https://www.huffpost.com/entry/zoom-tracks-not-paying-attention-video-call_l_5e7b96b5c5b6b7d80959ea96.

[37] *Attendee attention tracking*, ZOOM HELP CENTER, https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking (last visited: Aug. 3, 2020).

In fact, online proctoring tools are profoundly unfair to certain groups of students. As this section will document, academic surveillance tools disadvantage several groups of students relative to their peers, making it more difficult for these students to demonstrate their academic skills and preparedness. Video surveillance penalizes students with disabilities, seemingly in violation of US accessibility laws, and stigmatizes a range of normal behavior. Facial recognition technology performs more poorly on dark-skinned, female, and older students, creating an alarming and unfair obstacle to students who must verify their identities using facial recognition before and during exams. Low income students are unfairly hobbled by academic surveillance's significant technological and testing environment requirements. Academic surveillance tools not only disregard students' basic rights to privacy, they disregard students' rights to a fair chance to demonstrate what they have learned, exacerbating existing inequalities between privileged and less privileged students.

A. Surveillance Technology is Unfair to Disabled Students and Stigmatizes a Range of Normal Behaviors

Under US law, students with disabilities are guaranteed certain accommodations to ensure the effectiveness and appropriateness of their schooling. The Individuals with Disabilities Education Act (IDEA) requires that public school children who receive special education services have an Individualized Education Plan (IEP), a schooling plan individualized for every child to address their individual educational needs by a team including the child's parents, teachers, and school staff.[38] At the college level, students with disabilities are protected by Title II (at public institutions) and Title III (at private institutions) of the Americans with Disabilities Act (ADA), as well as certain protections available under Section 504 of the Rehabilitiation Act of 1973.[39] These rights together protect students in different ways: from forbidding discriminatory admissions to allowing in-class aides to changing school policies and procedures where appropriate and necessary to improve educational access for students with disabilities. These protections constitute a clear mandate: colleges must make reasonable accommodations for students with disabilities. But academic surveillance technology alarmingly undermines the accessibility of education and the spirit of these laws. Of the higher education institutions polled by Educause, 26% said that they were using "online proctoring" products that did not meet their accessibility standards.[40] This places an enormous burden on students with disabilities to challenge their schools and advocate for themselves.

The students whom these softwares may falsely flag are almost too numerous to count. Students with learning disabilities,[41] students who practice self-stimulatory behavior,[42] students who

[38] *A Guide to the Individualized Education Program,* U.S. DEPARTMENT OF EDUCATION (July 2000), https://www2.ed.gov/parents/needs/speced/iepguide/iepguide.pdf.
[39] *See: Fact Sheet: The Rights of College Students with Disabilities*, PROTECTION AND ADVOCACY FOR PEOPLE WITH DISABILITIES, INC. (July 2018), https://www.pandasc.org/wp-content/uploads/2018/07/ADA-504-College-Students-7-18-1.pdf.
[40] Grajek, *supra.*
[41] 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/.
[42] Flaherty, *supra.*

are medically unable to sit still for prolonged periods of time,[43] students with facial tics,[44] students who must use the bathroom frequently due to a medical condition,[45] breastfeeding students,[46] students who must care for their children, students with visual or hearing impairments, and students who may need to to administer medication during a test[47] may be flagged over and over again for "suspicious" behavior by academic surveillance technology. To avoid the risk of academic penalties, they may be forced to disclose sensitive medical or personal information to their educational institutions and even to third-party academic surveillance tech providers.[48] To add insult to injury, this kind of academic surveillance technology uses software to restrict access to certain functions on a student's computer which may interfere with accessibility software used by students with disabilities to enable them to take their exams.[49]

B. Facial Recognition Technology Performs More Poorly on Darker-Skinned, Female, and Older Students

Facial recognition technology struggles to accurately identify non-white, female, and older faces.[50] As a result, dark-skinned, female, and older students are more likely to encounter trouble verifying their identities before and during online exams. This problem is not hypothetical: students with black or brown skin have reported that facial recognition technology used for ID verification by academic surveillance programs has failed to recognize their faces.[51] Students of color have been asked to "shine more light on their faces" to be recognized by the facial recognition AI.[52] They have even at times been completely unable to use certain mandated surveillance programs such as Proctorio because of the system's inability to recognize their faces.[53] Any system that disproportionately bars students from taking exams on the basis of their race, sex, or age is unacceptably biased and clearly unfair.

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] Swauger, *supra.*

[47] Joe Patrice, *Bar examiners Ask Applicants to Kindly Stop Being Diabetic For A Couple Days,* ABOVE THE LAW (Sept. 3, 2020, 10:47 AM), https://abovethelaw.com/2020/09/bar-examiners-ask-applicants-to-kindly-stop-being-diabetic-for-a-couple-days/.

[48] Flaherty, *supra*; Patil and Bromwich, *supra.*

[49] Flaherty, *supra* ("Twenty-six percent of institutions said they were using products that didn't meet their accessibility standards. Respondus was by far the most widely used product").

[50] Kade Crockford, *How Is Face Recognition Surveillance Technology Racist?*, ACLU (June 16, 2020) https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/.

[51] Rebecca Heilweil, *Paranoia about cheating is making online education terrible for everyone*, VOX RECODE (May 4, 2020) https://www.vox.com/recode/2020/5/4/21241062/schools-cheating-proctorio-artificial-intelligence; @Uhreeb, TWITTER (Sept. 7, 2020); https://twitter.com/uhreeb/status/1303139738065481728; Victoria Hudgins, *Bar Exams' Facial Recognition Deployment is Heightening Test Takers' Anxiety,* LAW.COM (Aug. 5, 2020, 10:30AM), https://www.law.com/legaltechnews/2020/08/05/bar-exams-facial-recognition-deployment-is-heightening-test-takers-anxiety/?slreturn=20200907171737.

[52] Jean Dimeo, *Online Exam Proctoring Catches Cheaters, Raises Concerns*, INSIDE HIGHER ED. (May 10, 2017) https://www.insidehighered.com/digital-learning/article/2017/05/10/online-exam-proctoring-catches-cheaters-raises-concerns.

[53] Swaguer, *supra.*

C. Academic Surveillance Tools Place Unreasonable Demands on Low-Income, Minority, and Rural Students, Disadvantaging them Relative to their Peers

When schools use academic surveillance tools, they increase students' internet and computer needs—disadvantaging low-income, minority, and rural students unless schools also meet these needs. Academic surveillance technology requires reliable and high-speed Internet access, up-to-date computer hardware including a functioning webcam and microphone, and a testing environment with sufficient space and quiet. These demands cannot be met by many students of color, low income students, rural students, and students with challenging family situations such as homelessness. Even before the COVID-19 pandemic and the increased prominence of online learning, a study on technology and the achievement gap found that one in five students surveyed struggled to use technology necessary for online learning due to broken hardware and connectivity issues.[54] These issues affect low-income students, students of color, and rural students disproportionately: 16.9 million American children lack home Internet access adequate for online learning, including one in three families earning under $50,000 a year, one in three Black, Latino, and Native American families, and two in five rural families.[55] In addition, roughly 1.5 million school-aged children in America were homeless (on the street, in a shelter or motel, or doubled up with another family) at some point during the school year.[56] Homeless shelters do not allow children to be left unattended while their parents go to work, forcing an impossible choice between parents' work and students' remote learning.[57] Children who have frequently-changing residences similarly struggle with Internet access and a lack of technology-literate adults to help them participate in online learning.[58] Students who cannot meet the computing requirements associated with online learning and online proctoring cannot keep up with school. Moreover, they risk being penalized for their inability to go to school: when children have simply logged out or missed remote learning classes, some schools have reported the children to social services agencies.[59] Advocates and lawyers report seeing this phenomenon almost exclusively in high-poverty communities of color, and not in wealthier, whiter communities.[60]

Even when low-income students meet the technological requirements associated with online learning, academic surveillance poses further barriers to learning. Academic surveillance routines

[54] Gonzales, A. L., Calarco, J. M., Lynch, T., *Technology Problems and Student Achievement Gaps: A Validation and Extension of the Technology Maintenance Construct*, 47:5 Communication Research 750 (2020).

[55] "Students of Color Caught in the Homework Gap," Futureready (July 2020) https://futureready.org/wp-content/uploads/2020/07/HomeworkGap_FINAL7.20.2020.pdf

[56] *Federal Data Summary, School Years 2015-2016 Through 2017-2018*, National Center for Homeless Education, UNC Greensboro (January 2020), https://nche.ed.gov/wp-content/uploads/2020/01/Federal-Data-Summary-SY-15.16-to-17.18-Published-1.30.2020.pdf.

[57] Cory Turner, Homeless families Struggle With Impossible Choices as School Closures Continue, NPR (Oct. 7, 2020, 5:00 AM), https://www.npr.org/2020/10/07/920320592/an-impossible-choice-for-homeless-parents-a-job-or-their-childs-education.

[58] Alexis McGillis, *The Students Left Behind by Remote Learning*, New Yorker (Sept. 28, 2020), https://www.newyorker.com/magazine/2020/10/05/the-students-left-behind-by-remote-learning.

[59] Bianca, Vázquez Toness, *Your Child's a No-Show at Virtual School? You May Get A Call From The State's Foster Care Agency*, Boston Globe (Aug. 15, 2020, 4:07 PM), https://www.bostonglobe.com/2020/08/15/metro/your-childs-no-show-virtual-school-you-may-get-call-states-foster-care-agency/?s_campaign=breakingnews:newsletter.

[60] Vázques Toness, *supra*.

sometimes require students to circle their room with a laptop to show a remote proctor their environment. Being forced to show a stranger their living conditions may cause students living in poverty great discomfort and distress – feelings that may directly affect a student's performance in an exam. Furthermore, online exams may be interrupted by children, siblings, parents, or other family members. Students living in multigenerational households or students who have primary caretaking responsibilities for children or elder family members may experience these interruptions far more frequently than their peers, leading to a higher chance that they get falsely flagged for "suspicious" behavior.

In addition, some students have been asked to pay out of pocket for the use of academic surveillance technology, posing a clear problem for low-income students. Students have been asked to pay surcharges for online classes, and when privacy-conscious students have requested alternatives to online proctoring such as live human proctoring, they have been asked to foot the bill.[61] These additional charges may make online education cost prohibitive for financially vulnerable students, reinforcing and potentially exacerbating barriers to education for low-income families.

D. Academic Surveillance Tools Generate a Data Trail of Suspicion, Justifying Their Continued Use and Placing Students Under a Cloud of Suspicion

Academic surveillance unfairly penalize a range of students—disabled students, darker-skinned, female, and older students, and low income students—but it doesn't stop there. By flagging a wide range of normal behaviors as worth investigating, academic surveillance technology creates a data trail of suspicion, and the deceptive impression that cheating behavior is rampant in online learning. This, in turn, justifies the continued deployment of surveillance technologies by educational institutions, resulting in a vicious cycle.

Compared to in-person proctors in traditional exam settings, academic surveillance programs are perilously prone to incorrectly identifying innocent behavior as "suspicious." Proctortrack, an online proctoring program based on the Transportation Security Administration's technology to scan airport security video footage for "abnormal" facial expressions, uses algorithms to flag supposedly abnormal student behavior, like talking to someone off-screen, as "suspicious."[62] It requires students to sit upright and remain directly in front of their webcams at all times, according to guidelines posted on the company's site.[63] Changes in lighting, stretching, looking away, or leaning down to pick up a pencil can flag a student's test as having a violation under these guidelines. Proctortrack categorizes each student as having high or low "integrity" based on the number of these instances of behavior it deems "suspicious." Algorithms, unlike in-person proctors, have a limited understanding of context: a student can be flagged as a cheater for speaking to someone off-screen several times during an exam, even though the student may be engaging in completely innocent and typical at-home behavior such as responding to a relative's question or to a doorbell or

[61] Singer, *supra.*

[62] *Id.*

[63] *How do I prepare my testing environment?*, VERIFICIENT TECHNOLOGIES, https://verificient.freshdesk.com/support/solutions/articles/1000165250-how-do-i-prepare-my-testing-environment- (last visited: Aug. 3, 2020).

phone ring. Indeed, on message boards, students claim to have been flagged for such behaviors as stretching to grab a pen or letting their eyes wander during a long exam.[64] One student wrote on the online message board Reddit about being accused by a professor of cheating during an Honorlock-proctored exam, because the student had trained their gaze off-screen for a prolonged period of time while working out a math problem by hand.[65] Another anecdote documented a student who sneezed into a Kleenex several times due to seasonal allergies and was repeatedly wrongly flagged for looking away while holding what appeared to be paper, behavior that was deemed suspicious by her academic surveillance program.[66] Even if live proctors dismiss many automatically flagged behaviors as innocent, the production of these flags in the first place places students under a cloud of suspicion and justifies the continued deployment of academic surveillance tools.

E. Academic Surveillance Tools Allow Unseen Proctors to Closely Surveil Students

When there is a live proctor incorporated into academic surveillance technology, this person can typically see, hear, and instruct the student but is not visible to the student. This creates a spying scenario with a vast power imbalance beyond the dynamic that is inherent to any student-proctor relationship. In a traditional exam setting, the student is often able to observe the proctor and control, or at least monitor, the information that the proctor gathers about the student based on observation. In the academic surveillance scenario, the student is stripped of this ability completely. The student is rendered even more relatively powerless by the fact that the proctor has access to the student's computer and its contents in a way that proctors in in-person exam settings do not.

As a result, academic surveillance technology is downright creepy—with real mental health implications for students who are forced to engage with these intrusive programs. On TikTok, students have posted videos about being relentlessly watched by proctors[67], "having a mental breakdown" during an exam[68], and crying[69] as the test timer ticks down. The added level of stress from being watched closely by a stranger during an exam can exacerbate debilitating test anxiety[70] that roughly 25% of undergraduate students suffer from.[71] Students who have used Examity say it feels much more unnerving and off-putting than in-person proctoring by a professor or TA, perhaps because they are being watched closer up, by a stranger, and in a place more private than a

[64] Harwell, *supra*.

[65] u/OpulentBag, Reddit, https://www.reddit.com/r/college/comments/bajjum/professor_has_accused_me_of_cheating/ (last visited: Aug. 3, 2020).

[66] 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.

[67] @nicole.rzepka, TikTok, https://www.tiktok.com/@nicole.rzepka/video/6805574351845477637 (last visited: July 25, 2020).

[68] @kiahkramer, TikTok, https://www.tiktok.com/@kiahkramer/video/6791158098791828742 (last visited: July 25, 2020).

[69] @www.chumbucket.gov, TikTok, https://www.tiktok.com/@www.chumbucket.gov/video/6783467502874742021 (last visited: July 25, 2020).

[70] *Test Anxiety*, American Text Anxieties Ass'n, http://amtaa.org/ (last visited: Aug. 3, 2020).

[71] Thomas, C. L., Cassady, J. C., and Finch, W. H. *Identifying severity standards on the cognitive test anxiety scale: cut score determination using latent class and cluster analysis*, 36 J. Psychoeduc. Assess. 492–508 (2018).

classroom.[72] Students who have used academic surveillance programs describe their experiences as "uncomfortable," "intrusive," and "sketchy." In fact, when Rutgers University mandated the use of Proctortrack in some online courses in 2015, a group of students revolted, circulating a petition against it that quickly collected over 900 signatures.[73] It is unacceptable for educational institutions that should be supporting and facilitating students' learning to instead force them to use invasive, disturbing academic surveillance tools that unnerve students and interfere with learning.

F. The Bar Exam

The bar exam is not easy under any circumstances, and, as a group of four law school graduates wrote in the Washington Post, "we are not in the best of times; we are in the worst of times."[74] For years, the bar has been accused of being a formalized gate-keeping device rather than an actual minimum-competency exam.[75] The former Dean of Stanford Law School, in need of a California license where she had one for New York and Massachusetts, failed the California bar in 2005 – *after* standing at the helm of Stanford Law.[76]

So when most states considered going on with the Bar exam in the midst of the COVID-19 crisis, law graduates were upset. With a few exceptions, in-person exams mostly did not go forward; when they did, more than one had an examinee test positive immediately after taking the exam.[77] The pivot to virtual exams seemed like a solution to virus concerns. In reality, online exams have been a disaster. Michigan's July 28, 2020 online bar exam, offered by ExamSoft, crashed during its administration.[78] Michigan wasn't the only state to have such failures, and as the legal blog *Above the Law* noted: "*any* bar applicant having to withdraw because the platform wouldn't work — especially for technical problems that were explicitly pointed out ahead of time — is an unacceptable breakdown."[79]

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

[73] *Stop Use of Proctortrack in Online Courses*, CHANGE.ORG, https://www.change.org/p/rutgers-university-stop-use-of-proctortrack-in-online-courses (last visited: Aug. 3, 2020).

[74] Donna Saadti-Soto, Pilar Margarita Hernández Escontrías, Alyssa Leader, and Emily Croucher, *Why This Pandemic Is A Good Time To Stop Forcing Prospective Lawyers To Take Bar Exams*, THE WASHINGTON POST (Jul. 13, 2020, 2:45 PM), https://www.washingtonpost.com/education/2020/07/13/why-this-pandemic-is-good-time-stop-forcing-prospective-lawyers-take-bar-exams/.

[75] Marsha Griggs, *Building a Better Bar Exam*, 7 Tex. A&M L. Rev. 1 (2019) ("With the UBE comes a shift in power that favors bar examiners over academic freedom. Legal educators now face the uphill challenge of equipping their students to pass the bar exam without surrendering the academic autonomy to determine what students need to learn to become lawyers.").

[76] James Bondler and Nathan Koppel, *Raising the Bar: Even Top Lawyers Fail California Exam*, WALL STREET JOURNAL (Dec. 5, 2005), https://www.wsj.com/articles/SB113374619258513723.

[77] Joe Patrice, *Bar Examinee Tests Positive for COVID After Leaving Last Week's Exam Feeling Ill*, Above the Law (Sept. 15, 2020, 11:17 AM) https://abovethelaw.com/2020/09/bar-examinee-tests-positive-for-covid-after-leaving-last-weeks-exam-feeling-ill/; Joe Patrice, *Bar Examinees Learn Another Test-Taker Tests Positive for COVID,* ABOVE THE LAW (Jul. 30, 2020, 10:23 AM), https://abovethelaw.com/2020/07/bar-examinees-learn-another-test-taker-tests-positive-for-covid/.

[78] Joe Patrice, *Today's Online Bar Exam… Has Crashed,* ABOVE THE LAW (Jul. 28, 2020, 12:20 PM), https://abovethelaw.com/2020/07/todays-online-bar-exam-has-crashed-michigan/?rf=1.

[79] Joe Patrice, *Like COVID-19, Online Bar Exam is a Disaster and Was Entirely Preventable,* ABOVE THE LAW (Oct. 6, 2020, 12:43 PM) https://abovethelaw.com/2020/10/like-covid-19-online-bar-exam-is-a-disaster-and-was-entirely-preventable/.

Online bar exams appear to have been unfair in predictable ways. One examinee, who described herself as dark-skinned, could not pass a facial recognition verification system administered by Examsoft and waited three days to hear back from the company—which offered her only a "baseline reset."[80] Another examinee got her period mid-exam and had to choose between going to the bathroom (leaving the camera's view and invalidating her exam) or staying seated for the remainder of the exam.[81]

The National Conference of Bar Examiners (N.C.B.E.) has not met these challenges head on, and neither have the Courts. The Illinois Supreme Court made the mind boggling decision to refuse to force ExamSoft to do a dry run of the bar exam, leaving exam takers crossing their fingers and toes that the program would not meltdown for them the way it did in nearby Michigan. The NCBE offered a pathetic, week-before-the-October-exam national survey claiming that 4 of 5 Americans support having an in-person or remote bar exam.[82]

In response, law school graduates have called for so-caled "diploma privileges," which would provide graduates provisional license to practice law until in-person testing can resume. When law graduates are not licensed (which the Bar exam controls), they can't practice law. These individuals may be in hundreds of thousands of dollars in debt, and the vast majority of graduates do not go to the white-shoe law firms in New York and Washington, D.C. but instead to smaller, lower-paying local firms, public defenders' offices, and in-house counsel jobs.[83] Keeping these individuals from obtaining the appropriate license to support themselves and their families makes them deeply vulnerable. Doing so in the middle of the pandemic is unconscionable.

Part IV: Academic Surveillance Technology Violates Student Privacy and Exposes Students to Security Risks

As we have seen, academic surveillance technology is unfair to vulnerable groups of students, creating equity concerns. It generates a data trail of ostensibly suspicious behavior, justifying the tools' continued deployment, forcing students to operate under a cloud of suspicion, and interfering with learning. This section levies a third serious charge against academic surveillance technology: it disregards students' most basic rights to privacy, and in doing so, poses a serious data security risk. Indeed, surveillance tools pose two distinct security risks. They generate and retain sensitive data about students, and they allow free access to students' personal computer files.

[80] *Id.*

[81] @CeceliaScheeler, Twitter (Oct. 6, 2020), https://twitter.com/CeceliaScheeler/status/1313519480803405833; Joe Patrice, *The Online Bar Exam Amounted to Two Days of Cruel Vindictiveness,* Above the Law (Oct. 7, 2020) https://abovethelaw.com/2020/10/the-online-bar-exam-amounted-to-two-days-of-cruel-vindictiveness/?rf=1.

[82] Karen Sloan, *Will Ocotber's Online Bar Exams Implode? Takers Request 'Stress Tests' to Find Out*, Law.Com (Sept. 4, 2020), https://www.law.com/2020/09/04/will-octobers-online-bar-exams-implode-takers-request-stress-tests-to-find-out/; National Conference of Bar Examiners, National Survey Finds Support for Bar Exam (Sept. 30, 2020), https://www.ncbex.org/news/national-survey-bar-exam/.

[83] Ilana Kowarski, *See the Price, Payoff of Law School Before Enrolling*, US News (Mar. 18, 2020, 8:00 AM), https://www.usnews.com/education/best-graduate-schools/top-law-schools/articles/law-school-cost-starting-salary#:~:text=Starting%20Salaries%20for%20Law%20School%20Graduates&text=Among%20the%20181%20ranked%20law,to%20a%20high%20of%20%24190%2C000.

In March 2020, UC Santa Barbara faculty members who recognized these dangers criticized ProctorU in a letter opposing their school's use of the program due to concerns about ProctorU collecting data on students and making the data available to third parties, violating students' right to privacy and transforming the university from educational institution to surveillance tool.[84] Citing overall student privacy concerns and those of undocumented students in particular, the campus's Faculty Association Board wrote, "[w]e recognize that in our collective race to adapt our coursework and delivery in good faith, there are trade-offs and unfortunate aspects of the migration online that we must accept. This is not one of them."[85] ProctorU shot back in an aggressive response[86] that the Foundation for Individual Rights in Education publicly condemned.[87] As this heated back-and-forth demonstrates, academic surveillance programs are highly controversial to those who care not only about issues of equity, bias, and student well-being, but also about privacy and data security—and with good reason.

To begin with, students who use academic surveillance tools are often forced to do so by their academic institutions with weak, or more often non-existent, notice and consent procedures. Students are often given no timely notice that certain anti-cheating software will be used in their courses and for their assessments.[88] For example, Auburn University used Honorlock and ProctorU for virtually every test taken by the university's more than 23,000 undergraduates this year, regardless of whether students had previously consented to use of the technology or not.[89] Given the urgency with which classes and assessments moved online during the COVID-19 pandemic, students had no meaningful choice in the matter: they could either consent to the use of this software or otherwise lose a semester's worth of work and credit. In addition, professors often provide no back-up or alternative to students who are uncomfortable with academic surveillance technology, depriving students of a real chance to vet the technology for themselves and make an informed decision about using it.

Students also do not know what data is being collected about them, by whom this data is being collected, and for how long it is stored when they are essentially forced to use academic surveillance tools. Most proctoring programs record students' entire test sessions and store the audio and video recordings of these test sessions for at least days, often months, and sometimes years.[90] Often, proctoring companies' privacy policies include vague statements regarding data retention, such as "[w]e retain information for as long as necessary."[91] At a moment when millions of students are forced to study and take tests in crowded homes, this means that surveillance software not only

[84] Letter from U.C. Santa Barbara Faculty Ass'n to Henry Yang, Chancellor & David Marshall, Executive Vice Chancellor (Mar. 13, 2020) (https://cucfa.org/wp-content/uploads/2020/03/ProctorU_2020-1.pdf).

[85] *Id.*

[86] Letter from David Vance Lucas to UC Santa Barbara Faculty Ass'n (https://pubcit.typepad.com/files/bradley-bullying-letter.pdf).

[87] Paul Levy, *Can ProctorU Be Trusted With Students' Personal Data?*, PUBLIC CITIZEN (Mar. 25, 2020) https://pubcit.typepad.com/clpblog/2020/03/can-proctoru-be-trusted-with-students-personal-data.html.

[88] Singer, *supra.*

[89] Harwell, *supra.*

[90] *Honorlock Security and Privacy FAQ*, ST. PETERSBURG COLLEGE https://mycoursessupport.spcollege.edu/information-for-online-students/proctored-testing/honorlock/honorlock-security-and-privacy-faq.print (Mar. 25, 2020) (explaining that Honorlock stores student data for 12 months and sometimes longer.).

[91] *Privacy Policy,* PROCTORU, https://www.proctoru.com/privacy-policy (last visited: Aug. 3, 2020).

captures test takers in intimate settings and at stressful moments, they also record private family moments without the consent of other people in the environment who may be recorded involuntarily. This is tantamount to installing a school-issued surveillance camera in a family's living room.

The footage recorded and retained for prolonged periods of time by academic surveillance providers contains detailed identifiable and biometric information about students and those around them. Furthermore, academic surveillance providers reserve rights to retain, share, and reuse much of the data they gather from students' computers and bedrooms. For example, ProctorU, which oversaw two million tests last year from more than 750,000 students, states in its privacy policy for test-takers in California that the company shares an immense volume of sensitive student data with proctors and schools such as students' home addresses; details about their work; parental and citizenship status; medical records, including their weight, health conditions and physical or mental disabilities; and biometric data, including fingerprints, facial images, voice recordings and iris or retina scans.[92] Not only does ProctorU collect massive volumes of sensitive data about students, it also retains and uses the data in highly questionable ways. For example, it has edited the videos of students who are allegedly engaging in academic dishonesty into what it calls a cheating "Hall of Fame."[93]

Academic surveillance companies typically claim that they do not sell user data to third parties. However, typical privacy policies clearly indicate that they may share data for a variety of reasons, including for business purposes and to fulfill contracts with schools.[94] For example, Proctortrack claims to not share students' data with third parties and to delete it after 30 to 60 days, but its privacy policy states that the company may disclose users' personal information to third-party service providers or in the event of a company merger, sale, or bankruptcy.[95] PSI Online's privacy policy states that the company can share user data with law enforcement whenever it deems that necessary.[96] Terms such as these raise concerns that academic surveillance providers could turn into the eyes and ears of law enforcement in schools, violating the sanctuary policies[97] of many schools and reinforcing the school-to-prison pipeline.[98] At the very least, these companies share audio and video recordings of students with instructors so that they may vet the footage for academic integrity, creating significant new data collection and data sharing practices that did not exist before exams went online. Chris Dayley, the director of academic testing services at Utah State University, which uses Proctorio, describes the software as "spyware that we just legitimize."[99]

[92] *Privacy Policy California,* PROCTORU, https://www.proctoru.com/ca-privacy-policy (last visited: Aug. 3, 2020).
[93] Harwell, *supra.*
[94] Samantha Cleaver, *Online Test Proctoring Raises Privacy Questions Among University Faculty, Students,* DIGITAL PRIVACY NEWS (May 27, 2020) https://digitalprivacy.news/2020/05/27/proctoring/.
[95] *Privacy Policy*, VERIFICIENT TECHNOLOGIES, https://www.verificient.com/privacy-policy/ (last visited: Aug. 3, 2020).
[96] *Privacy Policy*, PSI TESTING EXCELLENCE, https://www.psionline.com/privacy/privacy-policy/ (last visited: Aug. 3, 2020).
[97] *Protecting Our Students and Their Families*, AMERICAN FEDERATION OF TEACHERS, https://www.aft.org/sites/default/files/plylertoolkit_sanctuary-safezone.pdf (last visited: Aug. 3, 2020).
[98] *School to Prison Pipeline*, NAACP LEGAL DEFENSE & EDUC. FUND, https://www.naacpldf.org/case-issue/school-prison-pipeline/(last visited: Aug. 3, 2020).
[99] Harwell, *supra.*

A second privacy issues is that academic surveillance services raise serious data security concerns. Many academic surveillance tools require giving third parties remote access to a student's computer screen, browser, webcam, and microphone. This creates a bad precedent for students' security habits by normalizing granting all-out access to one's devices. It also creates vulnerabilities that could result in malicious proctors or hackers exploiting remote access to students' computers, as by installing malware or spyware on students' computers or stealing or revealing sensitive student information to identity thieves.[100] Examity's privacy policy flatly states that the company does not guarantee the security of students' personal data. "Your transmission of data to our site is done entirely at your own risk," the privacy policy[101] reads, meaning Examity takes no responsibility for protecting the personal data of students, even though those students are obligated to provide their data to Examity to fulfill academic requirements. Again, this concern does appear to be merely hypothetical: for example, a student from Rose State College in Oklahoma explained that due to the use of an academic surveillance program by the school, "[s]ome people have been hacked [and it has] messed up their computers."[102] Students also have reason to fear aboveboard, or at least legal, sharing and selling of their data. There is insufficient legal protection against the sharing and selling of data because many academic surveillance services have condensed contracts[103] that expedite legal processes and mitigate liability concerns for the companies while sacrificing the legal protection of students and users.

Lastly, online proctors appear to be poorly supervised and poorly trained, increasing concerns about the security of students' files and sensitive personal data. In March, when much of the current test-taking panopticon was set up, concerns about violations of privacy and data security may have been overridden by a sense of urgency due to COVID-19. The final result, however, is worrisome, and worsened by the fact that no one is watching the student watchers. Academic surveillance employees have access to sensitive student data and files, but the evidence suggests that these employees are inadequately supervised and barely trained. Coronavirus-related lockdowns have forced some companies to allow their proctors to work remotely instead of in a supervised office, raising alarm among privacy advocates over who is gaining access to students' bedroom video streams.[104] Proctor training also falls short of companies' own expectations. Examity's website states that proctors must have "years of technical support accomplishments" and go through eight weeks of intensive training.[105] In reality, proctors' training, competence and experience leaves something to be desired: several proctors have admitted to having no prior proctoring experience, job listings for proctoring positions list only "good communication skills" as a requirement, and proctors have

[100] Chin, *supra.*

[101] *Privacy policy,* EXAMITY, https://examity.com/product-privacy-policy/ (last visited: Aug. 3, 2020).

[102] Sean Lawson, *Are Schools Forcing Students to Install Spyware That Invades Their Privacy As A Result of the Coronavirus Lockdown?*, FORBES (Apr. 24, 2020) https://www.forbes.com/sites/seanlawson/2020/04/24/are-schools-forcing-students-to-install-spyware-that-invades-their-privacy-as-a-result-of-the-coronavirus-lockdown/#45ede204638d.

[103] *Moving Courses Online During Covid-19*, HONORLOCK, https://honorlock.com/coronavirus/noclient/(last visited: Aug. 3, 2020).

[104] Harwell, *supra.*

[105] *Proctors | Auditors | Account Management*, EXAMITY, https://examity.com/proctors-auditors/(last visited: Aug. 3, 2020).

claimed that their training is not very intensive and lasts only a month.[106] Proctors' minimal supervision and training does not match the important task of safeguarding students' personal data.

Part V: Best Practices

The dangers posed by academic surveillance tools are well documented, and the need for these tools to supplement traditional methods of keeping students honest is not clear. As we have seen, academic surveillance systems exacerbate inequities that create an educational achievement gap for students with disabilities and others whose normal behavior is flagged as suspicious, for students of color, women, and older students who are marginalized by AI systems that cannot recognize their faces, and for low income students and others who cannot meet the technological requirements of academic surveillance tools. In their disregard for even basic rights to privacy, academic surveillance tools create significant risks for the security of student data. But the premise that academic surveillance tools are necessary to mitigate academic dishonesty during the COVID-19 pandemic is unsupported by facts.[107] Surveillance tools create a steady stream of data documenting ostensibly suspicious behavior, justifying their continued deployment, but little independent evidence suggests that online learning increases cheating—quite the opposite.

Given the risks associated with academic surveillance tools and the absence of evidence that they are needed to ensure academic integrity, educational institutions should refuse to use academic surveillance tools completely. Some schools have already done this, including the University of California at Berkley, which cited privacy and accessibility concerns when it rejected academic surveillance in April 2020.[108] If schools do use academic surveillance tools, they must opt for the least invasive technology possible by avoiding biometric monitoring, requiring third party verification of claims of efficacy, and auditing systems for the kinds of unfairness and bias discussed earlier in this report.

Honor codes have long been used as tools to ensure academic integrity in K-12[109] and higher education[110], and there is ample evidence that they are in fact effective in achieving this goal.[111] One review of the relevant literature demonstrated that because honor codes create a culture of academic integrity, the belief by students that their peers are cheating is lowered; this belief fosters cheating behaviors from students, so lowering it lowers incidendences of cheating.[112] Furthermore, the mere existence of an honor code creates the perception that schools have more severe penalties for cheating.[113] Rather than making students turn on each other as one might expect, this fosters a

[106] Chin, *supra*.
[107] Callahan, *supra*.
[108] Olivia Buccieri*, Online exam proctoring no longer allowed for UC Berkeley classes*, DAILY CALIFORNIAN (Apr. 5, 2020) https://www.dailycal.org/2020/04/05/online-exam-proctoring-no-longer-allowed-for-uc-berkeley-classes/.
[109] Camille M. Bertram, *Honor Codes Inspire Student Independence*, BERTRAM GROUP https://thebertramgroup.com/news/honor-codes-inspire-student-independence.
[110] *Honor Code*, STANFORD OFFICE OF COMMUNITY STANDARDS, https://communitystandards.stanford.edu/policies-and-guidance/honor-code (last visited: Aug. 3, 2020).
[111] Tatum, H. & Schwartz, B. M., *Honor Codes: Evidence Based Strategies for Improving Academic Integrity,* 56:2 THEORY INTO PRACTICE 129 (2017).
[112] *Id.*
[113] *Id.*

"strong and trusting" relationship between educators and their students.[114] Thus, a well thought-out honor code[115] that reinforces mutual respect between instructors and students and is enforced with real consequences for violations can lead to results that are on par with, if not more effective and certainly morally superior to those achieved by using academic surveillance tools.[116] Honor codes can ensure academic integrity without violating student privacy and aggravating inequities in educational achievement. They are viable alternatives to academic surveillance tools, and schools should deploy honor codes instead of resigning themselves to spying on students.

Another alternative to employing suspect academic surveillance tools to ensure academic integrity is to move away from traditional, closed-book and time-restricted exams, transforming the way schools think about assessing student learning. Closed-book and time-restricted exams are not the only effective methods of assessment, or even the most successful ones in measuring how well a student has internalized new knowledge.[117] Even before the COVID-19 pandemic and the mass exodus from campuses onto online platforms, institutions were considering alternative assessments to replace traditional exams. For example, the University of Maryland University College moved away from proctored exams, opting to use scenario-based projects to assess student learning instead.[118] A report by the Rochester Institute of Technology documents a variety of ways to assess students, including participation in discussions, low-stake quizzes, writing assignments, and real-time feedback on classroom activities.[119] For instructors who want to retain a traditional exam format, creative measures can prevent unwanted behavior without violating students' right to privacy. For example, using a deep question bank with randomized variables, each student can receive a different but comparable exam.[120] Andrew Robinson, an instructor at Carleton University who uses this method with success in 400-student physics classes, adds online assignments and participation scores from clicker use to assess student competence.[121] There are ample opportunities to design effective online assessments that encourage academic honesty without resorting to academic surveillance tools.

If educational institutions choose to use academic surveillance services despite the existence of viable alternatives and notwithstanding surveillance tools' negative impact on fairness and equity, students' well-being, and students' privacy and data security, they should do so with caution. Programs that generate and retain sensitive student data, including biometric data, should be avoided. Programs that allow unnecessary access to student files should be rejected. Programs that

[114] *Id.*
[115] *Best Practices: Remote Examinations*, Berkeley Center for Teaching & Learning, https://teaching.berkeley.edu/best-practices-remote-examinations (last visited: Aug. 3, 2020).
[116] Callahan, *supra.*
[117] *See:* Peter Tait, *'Intelligence Cannot be Defined by Exams,'* The Telegraph (Jun. 17, 2020), https://www.telegraph.co.uk/education/educationopinion/11678216/Intelligence-cannot-be-defined-by-exams.html.
[118] Mark Lieberman, *Exam proctoring for online students hasn't yet transformed*, Inside Higher Ed (October 10, 2018) https://www.insidehighered.com/digital-learning/article/2018/10/10/online-students-experience-wide-range-proctoring-situations-tech.
[119] *Teaching Elements: Assessing Online Students*, Rochester Inst. of Tech., https://www.rit.edu/academicaffairs/tls/sites/rit.edu.academicaffairs.tls/files/docs/TE_Online%20Assessmt.pdf (last visited: Aug. 3, 2020).
[120] Flaherty, *supra.*
[121] *Id.*

use bias-ridden artificial intelligence systems, such as automatic flagging of suspicious behavior and facial recognition, should be rejected: these programs are unfair to a host of students on the basis of disability, skin color, sex, and age, and they stigmatize a wide range of normal behaviors.

When institutions do adopt academic surveillance tools, they must ensure that these tools are continuously vetted by independent, expert third parties for efficacy, bias, and adequate data security policies. To do otherwise is to fail the promise they have made to students and their parents to make educational access for all students a priority. Schools and universities shirk their enormous responsibility to educate when they deny the invasiveness of the academic surveillance tools rather than acknowledging, addressing and minimizing the tools' risks. If schools judge that using these tools is absolutely necessary, they owe it to students to opt for the simplest, least invasive versions of the products available. Schools should choose the most stripped-down versions of surveillance tools, which usually consist of lockdown browser software that prevents students from leaving an exam website and opening other webpages or accessing other programs during an exam. Schools should avoid comprehensive surveillance packages that include intrusive AI and biometric tracking technology. Students are learners, thinkers, and citizens in training, not captives or offenders. Schools owe it to students to treat them accordingly by forswearing or minimizing academic surveillance.

Surveillance Technology Oversight Project, Inc.

40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT