SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Law Review

Volume 74 | Issue 3 Article 6

2024

Legal Implications of Remote Exam Proctoring: Extending Federal Law to Protect Student Privacy

Addie Griffey

— Note —

The Legal Implications of Remote Exam Proctoring: Extending Federal Law to Protect Student Privacy

Contents

INTRODUCTION

Place yourself back in your most stressful school course, as you are about to take your most important exam. The pressure you felt that day to perform well was likely high, motivating you to do your very best work. Now, imagine that instead of completing that exam in the typical classroom setting, you are forced to take the exam from a remote location, on the computer, while an invisible but all-seeing proctor or algorithm uses your webcam to track your every move, flagging any activity—a spare glance away or movement—that may indicate academic dishonesty but might be entirely benign. Further, imagine that this algorithm or proctoring software not only tracks your movements during your exam window but also records this highly personal and valuable biometric information and stores it for future uses and for durations unknown to you, the examinee.

While this sounds like an Orwellian[1] prediction of some future state, this is the reality many students found themselves in during and after the COVID-19 pandemic. Though remote proctoring software provides an opportunity for students to complete examinations online, while providing educational institutions a method for ensuring that students are complying with academic-integrity requirements, both the proctoring process and the proctoring companies' collection and storage of sensitive data present significant student-privacy concerns.

This Note explores dual privacy issues—unreasonable search and data security concerns—resulting from the use of remote proctoring technologies and examines the current legal remedies available to students whose privacy has been infringed, such as Fourth Amendment protections and state biometric information privacy laws. This Note will argue that the Fourth Amendment and current state privacy laws are insufficient to address these privacy issues and that supplementary solutions are necessary to fill the gaps present in these current remedies. It will suggest that in addition to the Fourth Amendment protections[2] for public university students, state privacy laws against recording in

1. *See* Shawn Hubler, *Keeping Online Testing Honest? Or an Orwellian Overreach?*, N.Y. TIMES (May 10, 2020, 5:00 AM), https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html [https://perma.cc/YDJ2-LMUP].

2. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

private spaces and privacy tort claims would serve as meaningful sources of protection against unreasonable searches through recordings conducted as part of the remote proctoring process. Additionally, this Note suggests that the Family Educational Rights and Privacy Act[3] should be amended to provide more comprehensive protection for student biometric information by incorporating provisions of state biometric-information and privacy laws. Both recommendations would provide additional privacy protection for students.

Part I of this Note describes the variety of remote-proctoring program types and both the privacy- and non-privacy-related legal consequences resulting from the use of these proctoring programs. Part II explains the current federal and state privacy protections available to students that potentially provide some remedy for the legal ills presented by remote proctoring technology.

Part III discusses the gaps in current student-privacy protections and advocates for remedies that will help fill those holes. Part III contends that the Fourth Amendment protects students at public institutions from unreasonable searches as part of their remote test-taking experience and further suggests the creation of state privacy laws, or the use of privacy tort remedies, to protect students' privacy, regardless of whether they attend a public or a private institution. Part III additionally proposes a federal student-privacy statutory remedy that would incorporate aspects of existing state and federal privacy laws to provide students greater access to information regarding the use of their biometric data and a right of action against entities who misuse that data. This remedy would allow students more comprehensive privacy protection against educational institutions and private companies alike.

I. REMOTE EXAM PROCTORING AND ITS CONSEQUENCES

In March 2020, colleges and universities across the United States began to close their campuses and move instruction online due to the COVID-19 outbreak.[4] These closures impacted over 14 million college students across the nation.[5] As instruction moved online, virtual exam proctoring software use increased exponentially—with one proctoring company, Proctorio, stating that its customer list grew over 500 percent from 2019 to 2021 and that it had "administered an estimated twenty-

3. 20 U.S.C. § 1232g.

4. Abigail Johnson Hess, *How Coronavirus Dramatically Changed College for Over 14 Million Students*, CNBC: MAKE IT (Mar. 26, 2020, 2:07 PM), https://www.cnbc.com/2020/03/26/how-coronavirus-changed-college-for-over-14-million-students.html [https://perma.cc/2E9T-PWWA].

5. *Id.*

one million exams in 2020, compared with four million in 2019."[6] While some educators have refused to implement remote proctoring services to monitor student conduct during online exams, the majority of educational institutions use the software to maintain academic integrity.[7]

There are several types of exam proctoring software offered by a variety of companies. These varieties include: "passive monitoring," which merely tracks the programs and applications accessed by students during an exam; "active restriction" or disabling of access to unnecessary or unapproved software on examinees' computers during the exam; "passive video surveillance," which requires examinees to complete their exams with their webcam on and records the exam session to be reviewed either by a human proctor or an artificial-intelligence program to detect any dishonest behavior; and "active video surveillance," which requires examinees to complete exams with their webcam on while a proctor watches in real time, and a recording may or may not be made.[8] This Note will focus primarily on the "passive video surveillance" variety, but similar analysis would apply to "active video surveillance" that includes recording the exam session.

While the COVID-19 pandemic and closure of educational institutions necessitated virtual instruction and, therefore, created an apparent need for mechanisms to monitor remote exam takers for academic dishonesty, many students have expressed their discomfort and dislike for these programs, citing both privacy- and non-security-related concerns.

6. Nora Caplan-Bricker, *Is Online Test-Monitoring Here to Stay?*, NEW YORKER (May 27, 2021), https://www.newyorker.com/tech/annals-of-technology/is-online-test-monitoring-here-to-stay [https://perma.cc/NPZ7-MFLZ]. Other proctoring companies experienced similar growth. ProctorU explained it had administered 2.5 million more exams in 2020 than in 2019, and Examity stated that its growth in 2020 "exceeded pre-pandemic expectations by thirty-five per cent [sic]." *Id.*

7. Sara Morrison & Rebecca Heilweil, *How Teachers Are Sacrificing Student Privacy to Stop Cheating*, VOX (Dec. 18, 2020, 9:30 AM), https://www.vox.com/recode/22175021/school-cheating-student-privacy-remote-learning [https://perma.cc/4BQV-SGCE]. While remote proctoring has declined since in-person education has resumed, schools continue to use the technology. Itzel Luna, *California Colleges Still Use Remote Proctoring Despite Court Decision*, CAL MATTERS (Feb. 27, 2023), https://calmatters.org/education/higher-education/college-beat/2023/02/remote-proctoring-california-colleges [https://perma.cc/JR7Q-QKD9].

8. Teresa Scassa, *The Surveillant University: Remote Proctoring, AI, and Human Rights*, 8 CAN. J. COMPAR. CONTEMP. L. 271, 280–82 (2022).

A. Privacy-Related Concerns Related to Remote Proctoring Software

While some educational institutions and educators find remote proctoring helpful and necessary, students often find it invasive and intrusive upon their personal spaces; they also cite concerns about how their data is collected, stored, and used.[9]

1. Unreasonable Search

The U.S. Constitution protects people from unreasonable search and seizure conducted by the government without a warrant issued upon finding probable cause. The text of the Fourth Amendment specifically protects "[t]he right of the people to be secure in their persons, houses, papers, and effects."[10]

Remote proctoring programs often require examinees to complete "room scans" that require students to use their webcams to show that their surrounding testing environments are void of any study aids or other materials the students may use to cheat.[11] Some institutions' remote-testing instructions require students to take their exams in a secluded location where they will not be interrupted.[12] For some students, especially those living at home or with other people, the only suitable testing location in their home is a bedroom.[13] Thus, when required to conduct a room scan prior to an examination, these students are forced to provide remote-proctoring companies the opportunity to

9. *See, e.g.*, Caplan-Bricker, *supra* note 6; Morrison & Heilweil, *supra* note 7; Anushka Patil & Jonah Engel Bromwich, *How It Feels when Software Watches You Take Tests*, N.Y. TIMES (Sept. 30, 2020, 1:42 PM), https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html [https://perma.cc/Y89V-7G8V]; Amanda Holpuch & April Rubin, *Remote Scan of Student's Room Before Test Violated His Privacy, Judge Rules*, N.Y. TIMES (Aug. 25, 2022, 4:42 PM), https://www.nytimes.com/2022/08/25/us/remote-testing-student-home-scan-privacy.html [https://perma.cc/YA3A-KUSH]; Shawn Hubler, *Keeping Online Testing Honest? Or an Orwellian Overreach?*, N.Y. TIMES (May 10, 2020, 5:00 AM), https://www.nytimes.com/2020/05/10/us/online-testing-cheating-universities-coronavirus.html [https://perma.cc/M79Y-HRD6].

10. U.S. CONST. amend. IV.

11. Shea Swauger, *Software That Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy*, MIT TECH. REV. (Aug. 7, 2020), https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/ [https://perma.cc/4AYP-FGST]; Ogletree v. Cleveland State Univ., 647 F. Supp. 3d 602, 608 (N.D. Ohio 2022), *vacated, appeal dismissed sub nom.* Ogletree v. Bloomberg, No. 22-3795, 2023 WL 8468654 (6th Cir. Dec. 4, 2023).

12. *Ogletree*, 647 F. Supp. 3d at 609; Patil & Bromwich, *supra* note 9.

13. *See Ogletree*, 647 F. Supp. 3d at 609.

view and record their most personal and intimate space—their bedroom.

However, when room-scan orders are required for public-university exams, this forced scan of a private space is not a harmless check to promote academic integrity. Rather, as a chemistry student from Cleveland State University alleged in a case discussed in Part II, such room scans are a form of unreasonable government search, prohibited by the Fourth Amendment.[14]

And while this student only challenged her public university's requirement of scanning her personal, private space, there is potentially opportunity to extend this unreasonable search argument beyond just room scans to include the forced recording of a student's person. Proctoring software that requires the use of a webcam records the face and upper body of each examinee during the duration of the exam to monitor for movements that indicate cheating or suspicious behaviors.[15] Some proctoring software utilizing artificial intelligence will flag instances of this suspicious conduct and will alert the professor to review the recording to analyze these behaviors, permitting professors in some cases to access and even download these student recordings to their personal computers.[16] Thus, the act of requiring students to submit to a recording of their person while taking their examinations in private spaces, and preserving the recording to possibly be viewed by instructors and others, likely constitutes an "unreasonable search" violating the Fourth Amendment.[17]

2. Data Security and Data Misuse

In addition to the concerns students have expressed regarding the room-scan aspect of remote exam proctoring, students have also voiced concerns about the storage and use of the data that proctoring companies collect.[18] During the remote exam sessions, proctoring companies collect a significant amount of personal data from test takers including "video, audio, keystroke patterns, and other biometric

14. *Id.*

15. 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/ [https://perma.cc/E8J3-5BVE].

16. Swauger, *supra* note 11.

17. *See infra* Part II.A.1.

18. Zoe Harwood, *Surveillance U: Has Virtual Proctoring Gone Too Far?*, YR MEDIA, https://interactive.yr.media/has-virtual-proctoring-gone-too-far/ [https://perma.cc/RTC7-37CU].

data."[19] Biometrics are defined as "measurements related to a person's unique physical characteristics, including but not limited to fingerprints, palmprints, voiceprints, facial, retinal, or iris measurements, and more."[20] These biometric data points "can be used as unique identifiers."[21] However, unlike traditional unique identifiers (such as Social Security numbers), the physical or behavioral sources of these data points cannot be replaced or reinvented, which is concerning to students who are subject to remote proctoring.[22]

Students have additionally articulated their worries that the proctoring companies' collections of personal data are vulnerable to cyberattack.[23] Students' concerns in this regard are valid. In 2020, two prominent proctoring companies, ProctorU and ProctorTrack, both experienced data-security events that put test-taker information at risk. In July of 2020, hackers published over 400,000 student records kept by ProctorU.[24] Later the same year, the parent company of ProctorTrack, an "advanced remote online proctoring solution" that "verifies [examinee] identities through face or 'knuckle scan,'" suspended its operations for over a week after hackers published part of the company's source code and sent offensive emails that appeared to come from the company to prior users.[25]

After the ProctorU data breach in 2020, university students filed a class action lawsuit against ProctorU under the Illinois Biometric Information Privacy Act (BIPA).[26] The students alleged that while they

19. *In re Online Test Proctoring Companies*, ELEC. PRIV. INFO. CTR., https://epic.org/documents/in-re-online-test-proctoring-companies/ [https://perma.cc/9WD6-BXZ5].

20. *Is Biometric Information Protected by Privacy Laws?*, BLOOMBERG L. (May 3, 2023), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/ [https://perma.cc/TCS9-FCP3].

21. *Id.*

22. Harwood, *supra* note 18.

23. 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/ [https://perma.cc/M977-WFHR].

24. *Id.*

25. *Id.*; *see also Proctortrack Resuming Service Following Comprehensive Cybersecurity Audit to Address Recent Security Incident*, PROCTORTRACK (Oct. 21, 2020, 10:25 PM), https://www.proctortrack.com/blog/announcement/proctortrack-resumes-its-services/ [https://perma.cc/274K-TTKK].

26. 740 ILL. COMP. STAT. 14 (2022); Kirsten Errick, *Students Sue Online Exam Proctoring Service ProctorU for Biometrics Violations Following Data Breach*, L. ST. (Mar. 15, 2021), https://lawstreetmedia.com/news

were using ProctorU's proctoring software, the company collected their biometric information "including eye movements and facial expressions (i.e., face geometry) and keystroke biometrics."[27] The students specifically alleged that ProctorU "failed to provide the requisite data retention and destruction policies, and failed to properly 'store, transmit, and protect from disclosure'" student biometric information.[28] The students further alleged that because ProctorU failed to take these steps, they were subject to a data breach, exposing the records of nearly 500,000 students.[29] The students further claimed that the ProctorU data breach included records dating back to 2012 and argued that this showed the company had retained the biometric data longer than necessary, violating BIPA.[30]

Other Illinois university students have brought similar actions against proctoring companies and their universities, making similar claims that these private entities violated BIPA in their collection, storage, and use of students' biometrics and failed to publish proper retention policies.[31]

Some proctoring companies address the inherent security risks present in data collection related to remote exam proctoring. For example, in its privacy policy, Meazure Learning, which acquired Examity in 2023,[32] cautions customers that though it limits access to personal information to third parties who need access to it to perform requested functions, it cannot guarantee that that information will be 100 percent secure and reminds customers that transmission of data to

/tech/students-sue-online-exam-proctoring-service-proctoru-for-biometrics-violations-following-data-breach/ [https://perma.cc/8CSJ-JAVZ].

27. Errick, *supra* note 26 (quoting Complaint ¶ 9, Thakkar v. ProctorU Inc., 571 F. Supp. 3d 927 (C.D. Ill. 2021) (No. 21-CV-2051)).

28. Complaint ¶ 2, *Thakkar*, 571 F. Supp. 3d 927 (No. 21-CV-2051).

29. *Id.* ¶ 41.

30. Errick, *supra* note 26.

31. *See* Patterson v. Respondus, Inc., 593 F. Supp. 3d 783, 795–96 (N.D. Ill. 2022); Duerr v. Bradley Univ., 590 F. Supp. 3d 1160, 1164 (C.D. Ill. 2022); Doe v. Nw. Univ., 586 F. Supp. 3d 841, 841–42 (N.D. Ill. 2022); *Thakkar*, 571 F. Supp. 3d at 931 (this case has since been moved to the United States District Court for the Northern District of Alabama, due to a forum-selection provision included in the terms of use provided by the proctoring company).

32. *Meazure Learning Strengthens Position as Global Leader of Assessment Solutions with Acquisition of Examity*, MEAZURE LEARNING (Sept. 6, 2023), https://www.meazurelearning.com/resources/meazure-learning-strengthens-position-as-global-leader-of-assessment-solutions-with-acquisition-of-examity [https://perma.cc/5J54-VBZQ].

its platform is done "at [their] own risk."[33] Students whose universities require the use of this type of proctoring software are left with little choice but to accept this risk, even if they would otherwise be unwilling to do so.

B. Nonprivacy Concerns Related to Remote Proctoring Software

While this Note does not focus on remediating any of the non-privacy-related consequences students subject to remote proctoring have faced, it is important to identify these consequences as additional sources for potential legal challenges related to remote exam proctoring. Students have raised a wide range of additional concerns regarding remotely proctored examinations, including disparate treatment of disabled or diverse examinees, increased anxiety amongst test takers, and malfunction or oversensitivity of proctoring software.[34]

1. Discrimination

Students have raised concerns that remote proctoring software presents challenges to certain test takers due to their race, disability, socioeconomic class, or family status. For instance, several students with darker skin tones have reported that the proctoring software, which requires that the test taker's face be identified before beginning the exam, was unable to recognize their faces.[35] In some instances, in order to have the software recognize them, students were forced to shine bright lights directly into their faces and keep those lights there for the examination period to ensure that the software would continue to recognize their faces.[36] Femi Yemi-Ese, a student at the University of Texas at Austin, explained that while the addition of the lights helped the proctoring software detect his face, it made it more difficult for him to not look away during the exam, creating another concern, as looking away is often flagged as indicative of cheating.[37]

33. *Privacy Policy*, MEAZURE LEARNING, https://www.meazurelearning.com/privacy-policy [https://perma.cc/4E2X-78HH].

34. *See* Patil & Bromwich, *supra* note 9; Caplan-Bricker, *supra* note 6; Monica Chin, *Exam Anxiety: How Remote Test-Proctoring Is Creeping Students Out*, THE VERGE (Apr. 29, 2020, 8:00 AM), https://www.theverge.com/2020/4/29/21232777/examity-remote-test-proctoring-online-class-education [https://perma.cc/L22Q-8WXA]; Harwood, *supra* note 18; Jason Kelley, *Stop Invasive Remote Proctoring: Pass California's Student Test Taker Privacy Protection Act*, ELEC. FRONTIER FOUND. (Mar. 24, 2022), https://www.eff.org/deeplinks/2022/03/stop-invasive-remote-proctoring-pass-californias-student-test-taker-privacy [https://perma.cc/N26K-ERHU].

35. Caplan-Bricker, *supra* note 6; Patil & Bromwich, *supra* note 9.

36. Caplan-Bricker, *supra* note 6.

37. *Id.*

In addition to extra difficulties for students of certain races, students who suffer from certain disabilities are also more likely to face challenges when using remote proctoring technologies. Video-recording software that utilizes artificial intelligence risks flagging disability-related movement or speech as suspicious activity typically thought to indicate cheating.[38] Because the software is designed to flag "atypical" movements or behaviors, and certain disabilities cause people to move in ways considered "atypical," persons affected by these conditions are more likely to be flagged by the software.[39]

For example, Sabrina Navarro, a student at California State University, Fullerton, had lived with a chronic tic disorder since childhood but had not registered it with her school's disability-services office as it had never affected her education.[40] However, once the COVID-19 pandemic hit, most of her courses required Proctorio virtual-exam-software use, and she feared that her involuntary mouth movements would get her flagged for academic dishonesty. So, Navarro obtained medical proof of her diagnosis to request accommodations. Still, Navarro feared the software would record her tics, which happened more frequently during high-stress situations like exams, and send these recordings to professors to review. The fact that her disability would be on display for her professors to review felt like an invasion of privacy to Navarro, who spent most of her life hiding her tic disorder.[41]

Further, remote proctoring instructions often require students to find quiet, undisturbed areas to complete their exams, as talking can be flagged as suspicious behavior.[42] However, for test takers who do not live alone, finding this secluded testing area could be difficult.[43] Additionally, students tasked with caring for other family members are also hurt by the secluded-environment requirement. One student, at the University of Texas at San Antonio, was forced to finish her freshman year remotely and move back home after in-person instruction was suspended during the pandemic. While learning from home, she also took care of her younger siblings. Frequently, during her remotely proctored exams, this student had to actively resist looking away from her screen while her siblings banged on the door seeking her attention.[44] Another student, at the University of Wisconsin, had a similar story.

38. Brown, *supra* note 15.

39. *Id.*

40. Patil & Bromwich, *supra* note 9.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

She claimed that Examity, the proctoring platform used by her instructor, made testing "especially difficult for parents" as it required students to test in an "empty, silent room." She was the mother of two young children and lived in a small home, so finding such a quiet space was a "tall order."[45]

Remote exam proctoring systems, while problematic for any student in some capacities, may present additional difficulties for students based on race, disability status, socioeconomic class, or familial status. These difficulties reflect the inadaptable nature of the remote exam proctoring technologies.

2. Increased Anxiety in Test Takers

Despite differences in race, socioeconomic class, or disability status, students from all backgrounds have claimed that remote proctoring technology has heightened their test-taking anxiety and left them feeling uneasy.[46] The use of a virtual proctoring system or known remote proctor could trigger anxiety in some students or exacerbate anxiety for students with underlying anxiety or post-traumatic stress disorders.[47] Still other students may feel additional anxiety due to technical difficulties related to the proctoring-software use. For example, Yemi-Ese, mentioned above,[48] was a college athlete who did not often feel stressed or anxious. However, after the remote proctoring technology failed to recognize his face and he was kicked out of an exam after his roommate made a loud noise in a separate room, he began experiencing feelings of anxiety. He tried to prevent himself from showing these feelings while testing, as he feared these physical signs of anxiety would cause the software to flag him for suspicious conduct.[49] Another student, at the University of British Columbia, Tiffany Chu, experienced significant anxiety when the link to her exam simply would not work on her laptop, and the proctoring company's support team was unable to resolve the issue.[50] Chu shared her challenges with the proctoring process on Reddit, an online discussion website, and noticed that other students posted that the proctoring software "made them anxious and miserable."[51]

45. Chin, *supra* note 34.

46. Harwood, *supra* note 18.

47. Brown, *supra* note 15.

48. *See supra* note 37 and accompanying text.

49. Caplan-Bricker, *supra* note 6.

50. *Id.*

51. *Id.*

Many students have shared that the remote proctoring experience feels much stranger than a typical in-class examination, and that it feels as if a professor is peering over their shoulder the entire exam, heightening the already-existing anxiety.[52]

3. Remote Proctoring Software Malfunction

While many educational institutions assert that remote proctoring systems are necessary to maintain academic integrity in the virtual education environment, there is evidence that these proctoring systems have flaws and err in flagging certain behaviors as suspicious when in fact no dishonesty has occurred. For example, in October 2020, California used ExamSoft proctoring services to administer its October bar exam.[53] Of the 8,920 applicants who took the exam online, nearly 36 percent were flagged for review.[54] The significant flagging of students was thought to be a result of technological issues, including an issue accessing the microphone within a certain brand of laptop, as many of those accused of cheating used that particular brand.[55]

Whether inadvertent flagging or malfunction is caused by differences in race, disability, or equipment type, the resulting issues call into question the reliability and usefulness of the remote proctoring system altogether. While not the topic of this Note, future discussion on the apparent prejudices and unreliability of exam proctoring software may be valuable.

II. Current Legal Protections for Privacy Issues Caused by Remote Proctoring

While there is no comprehensive student privacy legislation meant to address the exact problems created by the implementation and use of remote-proctoring software, there are current measures in place, at both the federal and state levels, that provide some privacy protections for students. These measures, however, leave significant gaps in coverage that leave some students vulnerable to having their personal privacy intruded upon or their highly sensitive data misused or retained.

52. *See* Chin, *supra* note 34; *see also* Harwell, *supra* note 23.

53. Stephanie Francis Ward & Lyle Moran, *Thousands of California Bar Exam Takers Have Video Files Flagged for Review*, ABA J. (Dec. 18, 2020, 2:15 PM), https://www.abajournal.com/web/article/thousands-of-california-bar-exam-takers-have-video-files-flagged-for-review [https://perma.cc/2ZWW-QXPP].

54. *Id.*

55. *Id.*; Kelley, *supra* note 34.

While students enrolled at public universities are likely protected from unreasonable searches in the form of room scans by the Fourth Amendment, those who attend private schools are not as clearly protected under existing legislation. Further, students whose data is collected by remote-proctoring companies while enrolled in both public and private universities do not have adequate protection over the use and storage of their personal biometric data. Although some states have enacted laws to address this issue, and the Federal Education Rights and Privacy Act (FERPA)[56] attempts to provide protection for student "records," additional protection is necessary to allow students to meaningfully police the practices of remote-proctoring companies and seek remedies when wronged.

A. Federal Protections

1. The Fourth Amendment

The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[57] In *Ogletree v. Cleveland State University*,[58] the United States District Court for the Northern District of Ohio granted summary judgment to a chemistry student at Cleveland State University who claimed that the remote room scans required by the proctoring software used by her[59] university for online

56. 20 U.S.C. § 1232g.

57. U.S. CONST. amend. IV.

58. 647 F. Supp. 3d 602 (N.D. Ohio 2022), *vacated, appeal dismissed sub nom.* Ogletree v. Bloomberg, No. 22-3795, 2023 WL 8468654 (6th Cir. Dec. 4, 2023). The United States Court of Appeals for the Sixth Circuit vacated this opinion and dismissed the appeals stemming from this opinion as moot in December 2023, after Ogletree passed away in February 2023, as upon her death, Ogletree lacked a "legally cognizable interest in the outcome of this case." *Ogletree*, 2023 WL 8468654, at *1. Though this opinion has been vacated, its logic was not "overruled" by the Sixth Circuit, and this Note refers to the logic and holding of this opinion to support its assertions as if it were not vacated, as students may raise similar challenges to mandatory room scans in the future.

59. Ogletree, a transgender woman, passed away in 2023. Prior to her death, she changed her name to "Amelia Ogletree," and the December 2023 Sixth Circuit order uses the pronouns "she" and "her" to refer to Ogletree. *See Ogletree*, 2023 WL 8468654, at *1. This Note uses the pronouns "she" and "her," consistent with Ogletree's obituary and the December 2023 court order. *Id.* at *1 n.*. The Northern District of Ohio's December 2022 opinion used Ogletree's prior name and pronouns. *See Ogletree*, 647 F. Supp. 3d at 606.

exams constituted unreasonable searches that violated the Fourth Amendment.[60]

Ogletree, who was living at home during the pandemic and was unable to take in-person courses at the time due to COVID-19 precautions and her own personal health circumstances, was taking an online exam when she was asked by the remote proctor to scan her testing environment with her webcam.[61] Because Ogletree was required to find a secluded place to test, she was forced to test from her bedroom, the only secluded space in her shared home.[62] Ogletree complied with the request and scanned her private bedroom as required.[63] This room scan and exam session were recorded and kept by Cleveland State University's exam proctoring vendor.[64]

Ogletree later alleged in federal court that Cleveland State University, a public higher-education institution, violated her Fourth Amendment rights.[65] She alleged that the university's policy of having proctors "conduct[] warrantless room scans of students' homes violat[ed] the Fourth Amendment's prohibition against unreasonable searches [applicable to] Ohio through the Fourteenth Amendment."[66] Ogletree asserted, and the court agreed, that students have a reasonable expectation of privacy in their homes and especially their bedrooms.[67]

The district court explained that "[a] Fourth Amendment search 'occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable'"[68] and held that Ogletree had a reasonable expectation of privacy in her home—particularly her bedroom—and that society recognizes that expectation as reasonable.[69] For "[a]t the Fourth Amendment's 'very core' lies 'the right of a man to retreat into his own home and there be free from unreasonable

60. *Ogletree*, 647 F. Supp. 3d at 608–09, 619–20.

61. *Id.* at 608–09.

62. *Id.*

63. *Id.* at 609.

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.* at 610.

68. *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).

69. *Id.* at 611 (explaining that modern Fourth Amendment jurisprudence examines one's "expectation of privacy in a particular place" and Ogletree's forced room scan occurred in her bedroom).

governmental intrusion.'"[70] The court held that this forced room scan was a search under the Fourth Amendment.[71]

Because the Fourth Amendment prohibits only "unreasonable" searches, the court next addressed whether the required room scans are reasonable.[72] While the Fourth Amendment "generally prohibits suspicionless searches," an exception may exist if the government intrusion serves a "special need[]."[73] The court then applied an existing test, adopted by the United States Supreme Court in *Vernonia School District 47J v. Acton*,[74] to determine whether the special need exception applied to Ogletree's case.[75] This test involves considering "(1) the nature of the privacy interest affected; (2) the character of the intrusion; (3) the nature and immediacy of the government concern; and (4) the efficacy of this means of addressing the concern."[76]

While the court recognized that the school had a legitimate interest in preserving the integrity of its exams, the other considerations weighed in the student's favor.[77] Ogletree's privacy interest in her own home was violated, and the protection of the home lies at the heart of the Fourth Amendment, whether the intrusion is virtual or physical.[78]

At the time the intrusion occurred, Ogletree had no other option but to take her course and exam online and was not notified that a search would be conducted until approximately two hours in advance of the exam. Although the scan was short in duration and Ogletree had some discretion as to where to direct her webcam, the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[79] Thus, the character of the intrusion also weighed in favor of Ogletree. Finally, the court noted that there were several alternative methods, not requiring a room scan, that would support the school's objective to "preserve the integrity" of its exams and that a "record of sporadic and discretionary use of room scans does not permit a finding that rooms scans are truly,

70. *Id.* at 611 (quoting Florida v. Jardines, 569 U.S. 1, 6 (2013)).

71. *Id.* at 614.

72. *Id.*

73. *Id.*

74. 515 U.S. 646 (1995).

75. *Ogletree*, 647 F. Supp. 3d at 614–15.

76. *Id.* at 615 (citing *Vernonia Sch. Dist.*, 515 U.S. at 654, 658, 660).

77. *Id.* at 615–17.

78. *See id.* at 615.

79. *Id.* at 616 (quoting Kyllo v. United States, 533 U.S. 27, 37 (2001)).

and uniquely, effective at preserving test integrity."[80] Thus, "the efficacy of the means" chosen weighed in favor of Ogletree.[81]

Based on its considerations of these factors, the court found that Cleveland State University's use of room scans as a part of its remote-proctoring procedures constituted an unreasonable search prohibited by the Fourth Amendment of the U.S. Constitution.[82]

While the holding in *Ogletree* likely would extend at least to similarly situated public-university students taking remotely proctored exams from their homes or other personal spaces, this protection would not extend to students enrolled at private universities, as the Fourth Amendment prohibits only unreasonable searches conducted by the government.[83] Thus, students at private universities are likely currently without clear legal recourse against their schools' room-scan policies.

2. Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a federal statute that affords all students who are eighteen or older, or enrolled in a postsecondary educational institution, the right to access, or seek to correct, their educational records and the opportunity to exercise some control over disclosure of their personally identifiable information from their educational records.[84]

The statute defines education records as "those records, files, documents, and other materials which—(i) contain information directly related to a student and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution."[85] In the rules interpreting this statute, "record" is defined as "information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche."[86]

FERPA applies to all educational institutions that receive funding from the Department of Education, including private postsecondary schools.[87] It generally prohibits these educational agencies or institu-

80. *Id.* at 616–17.

81. *Id.* at 617.

82. *Id.*

83. *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

84. *See* 20 U.S.C. § 1232g(d); *see also* 34 C.F.R. §§ 99.3, 99.10, 99.20 (2023) (explaining that students become "eligible students" when they reach eighteen years of age or enroll in a postsecondary education, and eligible students may seek to review their educational records and request that they be amended to correct inaccuracies).

85. 20 U.S.C. § 1232g(a)(4)(A).

86. 34 C.F.R. § 99.3 (2023).

87. *Id.* § 99.1.

tions from disclosing personally identifiable information from students' education records without consent.[88] Within this statute, "personally identifiable information" includes personal identifiers "such as the student's social security number, student number, or biometric record," and "biometric record" is defined as a record of a "measurable biological or behavioral characteristic[]" that can be used to recognize an individual.[89] Examples of these characteristics include "fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting."[90] An education institution or agency is permitted to disclose sensitive student information even without consent if the disclosure is made to "other school officials" who the education institution or agency determine have "legitimate educational interests" or other enumerated parties including officials from a school to which the student wishes to transfer, certain authorized representatives from U.S. governmental agencies, and law enforcement in certain circumstances.[91]

Because FERPA prohibits the disclosure of personally identifiable information, including biometric records, from student education records, which include video and audio recordings, this statute may apply to the disclosure of student biometric information collected during remote exam proctoring. Importantly, education records include those maintained by an educational institution or agency or by "a person acting for such agency or institution."[92] Because schools frequently contract with remote-proctoring companies to administer examinations and monitor students for them remotely, these proctoring companies are "acting for" the universities and thus likely are subject to FERPA.[93] This is significant because often recordings of students that are created during examinations are maintained by the proctoring companies and not the universities themselves.[94] Thus, without a

88. *See* 20 U.S.C. § 1232g(b)(1)–(2).

89. 34 C.F.R. § 99.3 (2023).

90. *Id.*

91. *See* 20 U.S.C. § 1232g(b)(1)(A)–(L).

92. *Id.* § 1232g(a)(4)(A).

93. *See* U.S. DEP'T OF EDUC., PRIV. TECH. ASSISTANCE CTR., RESPONSIBILITIES OF THIRD-PARTY SERVICE PROVIDERS UNDER FERPA, 1–2 (2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf [https://perma.cc/7UHG-7XFJ] (describing that schools often contract with third parties to "handle services they cannot efficiently provide themselves" and in these instances FERPA still governs the use and disclosure of personally identifiable information from education records).

94. *See generally, e.g.*, *Privacy Policy*, PROCTORTRACK (Aug. 24, 2023), https://www.proctortrack.com/privacy-policy/ [https://perma.cc/CHJ3-S4Z4]; *Frequently Asked Questions*, PROCTORIO, https://proctorio.com

finding that the proctoring software companies are "acting for" the universities, their improper disclosure of student biometric information would likely not be covered under FERPA. Students would only be able to seek legal recourse against education institutions if they themselves were improperly disclosing student videos or biometrics, rather than if the associated third-party proctoring companies were guilty of such disclosure. This, however, would provide legal recourse if school officials themselves were improperly disclosing recordings of students captured during the exam proctoring process as well.

Though FERPA appears to provide restraints on how biometric information collected through the remote exam proctoring process may be used and disclosed, the statute does not provide comprehensive privacy protections for student biometric data nor a meaningful remedy against entities that misuse or improperly disclose this data.[95]

B. State Protections

As the collection and use of biometric data has increased, states have introduced or enacted laws to prevent entities from collecting that data without proper disclosure and consent.[96] California has taken student privacy a step further and passed the Student Test Taker Privacy Protection Act,[97] which is aimed at regulating proctoring companies' collection, storage, use, and disclosure of students' personal information.[98] This measure joins the existing California Consumer Privacy Act of 2018,[99] which aims to protect consumer information and give consumers the right to know what information is collected, how it is used, and to whom it is disclosed. These state privacy laws are described in greater length throughout this Subpart.

1. State Biometric Privacy Laws

a. Illinois Biometric Information Privacy Act (BIPA)

In 2008, Illinois became the first state to pass a biometric-privacy law when the state legislature unanimously passed the Biometric Information Privacy Act (BIPA).[100] The Illinois legislature recognized

/faq [https://perma.cc/24QV-VT5H]; *What's After My Exam*, Meazure Learning + EXAMITY, https://www.examity.com/post-exam-steps/ [https://perma.cc/Y9KT-V53R] (describing proctoring platform retention practices).

95. *See infra* Part III.B.1.

96. *Is Biometric Information Protected by Privacy Laws?*, *supra* note 20.

97. CAL. BUS. & PROF. CODE § 22588 (West Supp. 2024).

98. *Id.*

99. CAL. CIV. CODE §§ 1798.100, 1798.110 (West 2022).

100. 740 ILL. COMP. STAT. 14 (2022); Eliza Simons, *Putting a Finger on Biometric Privacy Laws: How Congress Can Stitch Together the*

the growing use of biometrics in business and the significant security risks that come along with the ubiquity of collecting and storing unique, irreplaceable biometric information.[101] BIPA requires private entities that possess biometric information to develop and publish a written retention schedule and guidelines for destroying biometric information once the purpose for collecting the information has been satisfied, or at a maximum of three years since the person to which the information belongs last interacted with the entity, whichever is sooner.[102] Section 15(b) of BIPA prohibits private entities from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining biometric information unless they (1) inform the person in writing that biometric information is being collected or stored; (2) inform the person of the purpose for the collection and the length of time for which the biometric information will be stored and used; and (3) receive written consent[103] from the person whose information is to be collected or their lawful representative.[104] The Act also prohibits entities from selling, leasing, or otherwise profiting from biometric information and prohibits disclosure of that information without consent of the subject, unless required to complete a financial transaction authorized by the subject of the biometric information, or to comply with state or local law or valid subpoena.[105]

Section 15(e) requires all entities in possession of biometric information to use reasonable care in storing, transmitting, and

Patchwork of Biometric Privacy Laws in the United States, 86 BROOK. L. REV. 1097, 1112 (2021); *Biometric Information Privacy Act (BIPA)*, ACLU ILL., https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa [https://perma.cc/48YH-RRED].

101. 740 ILL. COMP. STAT. 14/5 (2022).

102. *Id.* at 14/15.

103. While this is an important protection for individuals, it may be less useful for students, for in the test-taking context, consent hardly appears to be freely given—students may be required to take examinations as part of their courses, and these required examinations may involve the use of proctoring technology that collects test-taker biometric information. To take remotely proctored exams, students must accept the proctoring software's terms and conditions, thereby consenting to its data-collection practices. *See, e.g.*, *Exam Day: What to Expect*, PROCTORU, https://support.proctoru.com/hc/en-us/articles/360043565051-Exam-Day-What-to-Expect [https://perma.cc/FW8W-XD7X]. As described below, the Texas Capture or Use of Biometric Identifier Act and Washington's Biometric Identifiers Act, like BIPA, also require that entities obtain individuals' consent before collecting their biometric information. *See infra* text accompanying notes 116 and 123.

104. *Id.*

105. *Id.*

protecting that information from disclosure. Additionally, the Act requires these entities to store, transmit, and protect this biometric information in a manner equally or more protective than the way the "entity stores, transmits, and protects other confidential and sensitive information."[106]

BIPA section 20 provides aggrieved individuals a private right of action against entities that violate the terms of BIPA.[107] It explains that a prevailing party may recover "liquidated damages of $1,000 or actual damages, whichever is greater" against noncompliant entities acting negligently; "liquidated damages of $5,000 or actual damages, whichever is greater," against noncompliant entities acting recklessly or intentionally; attorneys' fees and costs; and other relief, such as an injunction, when deemed appropriate.[108] In *Rosenbach v. Six Flags Entertainment Corp.*,[109] the Illinois Supreme Court held that a person need not allege any actual injury beyond a violation of his or her rights under BIPA in order to bring an action against a noncompliant company.[110] Thus, any person whose biometric information is collected, retained, or disclosed in violation of BIPA has standing to exercise the private right of action provided to aggrieved individuals in BIPA.[111]

In the following years, the Illinois state courts and federal district courts have seen several complaints filed under BIPA.[112] Most relevant to this Note, several Illinois university students have filed complaints against remote exam proctoring companies and private universities alleging BIPA violations.[113] These students claim that the remote-proctoring companies collect various forms of biometric data, including facial geometry, through students' webcams, and that the proctoring companies, and universities by contracting with these companies, violated BIPA by failing to receive consent to collect students' biometric information, improperly disclosing this information, or failing to comply with BIPA's retention-policy requirements.[114]

106. *Id.*

107. *Id.* at 14/20; Simons, *supra* note 100, at 1114.

108. 740 ILL. COMP. STAT. 14/20 (2022).

109. 129 N.E.3d 1197 (Ill. 2019).

110. *Id.* at 1199–1200, 1207.

111. Simons, *supra* note 100, at 1115.

112. *Id.*

113. *See* Patterson v. Respondus, Inc., 593 F. Supp. 3d 783, 783–84 (N.D. Ill. 2022); Duerr v. Bradley Univ., 590 F. Supp. 3d 1160, 1160–61 (C.D. Ill. 2022); Doe v. Nw. Univ., 586 F. Supp. 3d 841, 841 (N.D. Ill. 2022); Thakkar v. ProctorU, 571 F. Supp. 3d 927, 927 (C.D. Ill. 2021).

114. *See Patterson*, 593 F. Supp. 3d at 783–84; *Duerr*, 590 F. Supp. 3d at 1160–61; *Doe*, 586 F. Supp. 3d at 841; *Thakkar*, 571 F. Supp. 3d at 933.

b. Texas Capture or Use of Biometric Identifier Act

The Texas Capture or Use of Biometric Identifier Act (CUBI)[115] is similar to BIPA in several ways. Like BIPA, CUBI prohibits a private entity from capturing a "biometric identifier of an individual for a commercial purpose" unless the entity informs the individual before collecting the biometric identifier and receives the individual's consent to capture that data.[116] Additionally, CUBI prohibits private entities that possess biometric identifiers from selling, leasing, or disclosing the identifiers unless the individual gives consent, or the disclosure is necessary to complete a financial transaction requested by the individual or to comply with state or federal law or a valid warrant.[117] CUBI also requires that entities store and protect these biometric identifiers with reasonable care and in a manner equally or more protective than the manner in which the entity protects other confidential information.[118] Finally, the Act requires entities to destroy the biometric identifiers "within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires."[119]

The main difference between CUBI and BIPA is that CUBI does not provide for a private right of action to enforce its terms.[120] Rather,

---

Although beyond the scope of this Note, it is worth mentioning that due to an exception within BIPA for financial institutions subject to Title V of the Gramm-Leach-Bliley Act (GLBA) (15 U.S.C. §§ 6801–6809, 6821–6827), *Doe v. Northwestern University* and *Duerr v. Bradley University* were dismissed, as the district courts found that universities were financial institutions under the GLBA because they participate in federal student-aid programs. *See Duerr*, 590 F. Supp. 3d at 1171; *Doe*, 586 F. Supp. 3d at 842–44.

After *Thakkar* was transferred to the Northern District of Alabama, the district court dismissed the case, explaining that the plaintiffs' BIPA claims arose from ProctorU's Terms of Service, and per a choice-of-law provision, these claims were to be "governed by the laws of the State of Alabama," barring plaintiffs' Illinois BIPA claims. Thakkar v. ProctorU, Inc., 643 F. Supp. 3d 1304, 1311, 1315 (N.D. Ala. 2022). Respondus eventually agreed to settle its class-action BIPA case. Scott Holland, *$6.25M Deal to End Biometrics Class Action vs Online College Test Proctor Respondus Over Student Face Scans*, COOK COUNTY RECORD (June 22, 2023), https://cookcountyrecord.com/stories/644483545-6-25m-deal-to-end-biometrics-class-action-vs-online-college-test-proctor-respondus-over-student-face-scans [https://perma.cc/9VXR-WMU3].

115. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2023).

116. *Id.* § 503.001(b).

117. *Id.* § 503.001(c).

118. *Id.*

119. *Id.*

120. Simons, *supra* note 100, at 1117.

it explains that an entity that violates its terms is subject to a "civil penalty of not more than $25,000 for each violation" and that "[t]he attorney general may bring an action to recover the civil penalty."[121] In the following Subpart, this Note will argue that for effective enforcement and privacy protection for students, a private right of action is critical.

c. Washington Biometric Identifiers Statute

In 2017, after noting the concern regarding the increased collection of individuals' biometric information without their consent or knowledge, Washington passed the Biometric Identifiers Act,[122] intending "to require a business that collects and can attribute biometric data to a specific, uniquely identified individual to disclose how it uses that biometric data, and provide notice to and obtain consent from an individual before enrolling or changing the use of that individual's biometric identifiers in a database."[123] Washington's Act differs from BIPA and CUBI by specifying that only an entity that has "enrolled" biometric identifiers is subject to its provisions.[124] The Act defines "enroll" to mean "capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual."[125] Thus, it is unclear whether remote-proctoring companies would be subject to the terms of this Act, as its applicability depends on whether the companies manipulate the collected biometric identifiers in this particular way.

Entities that do "enroll" biometric identifiers for a commercial purpose must first provide notice, obtain the individual's consent, or provide "a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose."[126] Like CUBI and BIPA, the Washington Act prohibits covered entities from selling, leasing, or otherwise disclosing biometric identifiers for a commercial purpose without consent.[127] However, like CUBI and BIPA, the Act provides several instances when disclosure is permitted, such as when necessary to provide a product or complete a financial transaction that the individual requested, when required by law, or to prepare for litigation

121. § 503.001(d).

122. Ch. 299, 2017 Wash. Sess. Laws 1141 (codified at WASH. REV. CODE § 19.375 (2023)).

123. WASH. REV. CODE § 19.375.900 (2023).

124. *Id.* § 19.375.020.

125. *Id.* § 19.375.010(5).

126. *Id.* § 19.375.020(1).

127. *Id.* § 19.375.020.

or respond to the judicial process.[128] The Washington Act, however, also permits disclosure when it is "made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose" inconsistent with the Act.[129]

The Washington Act also lacks the private right of action provided in BIPA and instead may only be enforced "by the attorney general under the consumer protection act."[130] As Washington's Act is narrowly applied to only those entities that "enroll" biometric identifiers and is not enforceable by a private right of action, it is the "least inclusive" of the three states' biometric-privacy laws.[131] It is also perhaps the least helpful in redressing the harms students face related to the use of remote-proctoring programs.

2. California State Privacy Statutes

a. California Consumer Privacy Act

The California Consumer Privacy Act (CCPA)[132] is broader in scope than the state biometric-privacy acts discussed previously. It gives consumers more control over an array of personal information that businesses collect from them and includes biometric information within its definition of personal information.[133]

The CCPA requires businesses that collect consumers' personal information to disclose the categories of personal information collected, the purposes for which the information is gathered, and whether the information is sold or shared.[134] Additionally, consumers have the right to request that these businesses disclose the categories of the information collected, the categories of sources from which the businesses collected the data, the business purpose for collecting the information, the categories of third parties to whom the businesses disclose the data, and the specific pieces of information collected about the consumer.[135] Consumers may request that a business delete any personal information that it has collected, although the business may deny that request if it is reasonably necessary to maintain the consumer information to complete the transaction requested by the consumer, to comply with

128. *Id.*

129. *Id.*

130. *Id.* § 19.375.030(2).

131. Simons, *supra* note 100, at 1118.

132. Cal. Civ. Code §§ 1798.100–1798.199.100 (2022 & Supp. 2024).

133. *Id.* § 1798.140(v); Simons, *supra* note 100, at 1108.

134. § 1798.100(a)(1)–(2).

135. *Id.* § 1798.110(a).

the California Electronic Communications Privacy Act, to comply with a legal obligation, or for other limited purposes.[136] Businesses that sell or share consumer information must notify consumers of this practice and give them the opportunity to opt out of the sale or sharing of their personal information. Consumers may exercise their right to opt out or direct businesses not to sell or share their personal information at any time.[137] Under the CCPA, a business that receives direction from a consumer not to sell or share that consumer's personal data is prohibited from doing so until the consumer subsequently provides consent to sell or share the information.[138]

Consumers additionally have the right to request that businesses correct inaccurate personal information collected from them. Businesses that receive a verifiable consumer request for correction must make reasonable efforts to correct the information as requested by the consumer.[139] Consumers also have the right to direct a business that collects sensitive personal information about the consumer to limit the use of that information to that which is necessary to provide the goods or services requested by the consumer.[140] Sensitive personal information includes "[t]he processing of biometric information for the purpose of uniquely identifying a consumer."[141]

While the CCPA provides numerous rights to consumers intended to protect private information, it does not provide injured individuals with a private right of action against noncompliant businesses, except for limited recovery up to $750 under certain circumstances that result in a data breach.[142] Otherwise, consumers may report violations to the California Attorney General through a "consumer complaint."[143] If a violation is found, the noncompliant business may be issued an administrative fine of no more than $2,500 per violation, or $7,500 per violation if the violations are intentional. These fines will be assessed and recovered in an enforcement action brought by the California Privacy Protection Agency.[144] Under the CCPA, students are not specifically identified as a group requiring protection; in fact, proctoring

136. *Id.* § 1798.105(a), (d).

137. *Id.* § 1798.120(a).

138. *Id.* § 1798.120(d).

139. *Id.* § 1798.106(c).

140. *Id.* § 1798.121(a).

141. *Id.* § 1798.140(ae)(2)(A).

142. *See id.* § 1798.199.90(e) (referencing section 1798.150(a)(1)(A)).

143. *Frequently Asked Questions (FAQs)*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/faq.html#faq_res_1 [https://perma.cc/S9BX-HLH5].

144. § 1798.155(a).

companies have argued that schools or test administrators, not the students themselves, are consumers of their services, and thus students are not protected from proctoring companies' wrongdoings under the CCPA.[145]

b. Student Test Taker Privacy Protection Act

California's recently passed Student Test Taker Privacy Protection Act (STTPPA)[146] remedies the students-as-consumers issue by specifically regulating proctoring companies that operate in educational settings.[147] Specifically, the Act states that proctoring-services companies may only collect, use, retain, or disclose personal information strictly necessary to provide their proctoring services.[148] The Act applies the same definition of "personal information" used in the CCPA, so this definition of personal information includes biometric information.[149] Like state biometric-information statutes, the STTPPA contains exceptions that do not prohibit proctoring-services companies from collecting, using, retaining, or disclosing personal information to (1) comply with the law, a court order or subpoena, or a criminal, civil, or regulatory inquiry; (2) cooperate with law enforcement; or (3) exercise or defend a legal claim.[150]

While the STTPPA closes the potential loophole left open by the CCPA regarding protection of student data collected by proctoring companies, the Act does not provide a specific private right of action to students who have been injured by noncompliant proctoring companies—those that "collect, use, retain, [or] disclose" personal information beyond that "strictly necessary to provide [proctoring] services."[151] While it is unclear if the Act will be enforced in the same way as the CCPA, the STTPPA makes no explicit grant of a private right of action to students, leaving students without options for personal legal recourse.

145. Kelley, *supra* note 34.

146. Ch. 720, 2022 Cal. Stat. 8112 (codified as amended at CAL. BUS. & PROF. CODE § 22588 (West Supp. 2024)).

147. CAL. BUS. & PROF. CODE § 22588 (West Supp. 2024).

148. *Id.* § 22588(a).

149. *Id.* § 22588(c); *see also* CAL. CIV. CODE § 1798.140(v)(1)(E) (West Supp. 2024).

150. CAL. BUS. & PROF. CODE § 22588(b)(1)–(3) (West Supp. 2024).

151. *See id.* § 22588.

III. Expansion or Creation of Laws to Protect Students from Remote-Proctoring Harms

A. Surveillance Remedies

1. Continued Enforcement of the Fourth Amendment

Ogletree's Fourth Amendment analysis provides a helpful framework when determining the legality of forced room scans as part of remote exam proctoring procedures implemented by public school systems. However, the *Ogletree* court did not discuss the legality of forced recordings without room scans. There is opportunity to extend *Ogletree*'s holding beyond forced room scans to required recordings of test takers in private spaces.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[152] As explained in *Ogletree*, "[a] Fourth Amendment search 'occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'"[153] The court held that Ogletree had a subjective expectation of privacy in her home while taking her virtual exam, and that expectation is one that society considers reasonable and lies at the very center of the Fourth Amendment's protection against government intrusion.[154] The same logic can be applied to the forced recording of test takers, even apart from the room-scan portion. If students have a reasonable expectation of privacy in their homes and the Fourth Amendment protects the rights of people to be secure, not only in their property, but also in their persons, then a forced recording of students, in an area in which they have a reasonable expectation of privacy, meets the criteria laid out in *Ogletree* and constitutes a Fourth Amendment search.

The second part of the analysis would consider the same factors described in Part II—"(1) the nature of the privacy interest affected; (2) the character of the intrusion; (3) the nature and immediacy of the government concern; and (4) the efficacy of this means of addressing the concern"—to determine if the recording of the test taker, without suspicion, is unreasonable or if a special-needs exception applies.[155] If these factors were applied to test takers' webcam recordings, the same outcome would result as with the room-scan analysis conducted in *Ogletree*. The nature of the privacy interest affected would be just as

152. U.S. Const. amend. IV.

153. Ogletree v. Cleveland State Univ., 647 F. Supp. 3d 602, 610 (N.D. Ohio 2022) (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)), *vacated, appeal dismissed sub nom.* Ogletree v. Bloomberg, No. 22-3795, 2023 WL 8468654 (6th Cir. Dec. 4, 2023).

154. *Id.* at 610–11.

155. *Id.* at 615.

personal—a recording being captured of a student in a private space. The character of the intrusion would arguably be more significant than a room scan, as the recording of a room scan lasts only for a few seconds while a recording of the individual test taker would last the entirety of the exam. Finally, while the school has a legitimate interest in preserving academic integrity and recording students while testing helps accomplish that objective, there are alternatives available that would eliminate the need for recording test takers. The school could employ lockdown browsers to control students' internet and program access during the exam. Additionally, schools could utilize other test features such as a time limit per question, different-ordered questions, and a feature prohibiting students from returning to a question once they submitted their answer to help prevent unauthorized use of hard copy materials as well. Schools could also explore other assessment options, such as a written paper or project, which would not allow students to benefit from the same forms of academic dishonesty typically employed to cheat on exams (e.g., unauthorized use of notes or internet sources), and which could be subject to plagiarism-checking tools. For these reasons, the forced recording of virtual test takers during a remote exam could likely be seen as a Fourth Amendment violation.

2. State-Law Remedies

Unfortunately, students at private universities are unable to take advantage of these Fourth Amendment protections, as their universities are not considered state actors constrained by the Fourth Amendment. To afford private-university students the same privacy protections as those at public universities, states should adopt privacy laws to protect people within their states from unreasonable searches of their person or private spaces conducted by private entities, just as the Fourth Amendment protects persons from unreasonable government searches.

Several states have existing criminal laws that prohibit private persons from recording people, without their consent, in areas where they have a reasonable expectation of privacy. California law prohibits a private person from using a camera or recording device to view into a private space where the occupant has a reasonable expectation of privacy, including a bedroom, with the intent to invade the privacy of the occupant.[156] Other states, such as Michigan, Utah, South Dakota, and New Hampshire, have similar laws prohibiting the use of devices to observe or record sounds or events in a private place without the consent of the occupant.[157]

156. CAL. PENAL CODE § 647(j)(1) (West Supp. 2024).

157. *See* MICH. COMP. LAWS ANN. § 750.539d (West 2004); UTAH CODE ANN. § 76-9-402(2)(b)–(c) (LexisNexis Supp. 2023); S.D. CODIFIED LAWS § 22-21-1(2) (Supp. 2023); N.H. REV. STAT. ANN. § 644:9(I) (2016).

These existing recording statutes may provide an opportunity to protect students attending private universities from forced room scans and test recordings, at least when students take examinations from a private location, such as their home. Room scans and exam recordings involve the use of a web camera and are used to capture the images or record the events and sounds during the test period. This appears to fall under the protections granted in the Michigan, Utah, South Dakota, and New Hampshire statutes, and could perhaps even fall under the California statute's protection, if it is determined that the school required the room scan or exam recording to invade students' privacy. This prong would likely be more difficult to meet as the schools would likely explain that the recordings were conducted to protect the academic integrity of the exam, rather than invade students' privacy. However, the clear intention to monitor students may qualify as an intention to invade their privacy.[158]

Even if existing statutes like those in California, Michigan, Utah, South Dakota, and New Hampshire do not currently protect students from invasive exam recordings and room scans, they provide a strong foundation for such laws to be created and provide support for the assertion that people, including students, have a claim to privacy in their own homes and private spaces.

3. Tort Remedies

Even if states do not enact statutes protecting students from forced room scans or recordings conducted on behalf of their private universities, students may be able to find relief by bringing invasion of privacy tort claims, particularly for intrusion upon seclusion. The Second Restatement of Torts states that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[159] This form of invasion of privacy does not depend on actual publicity of the affairs of the person whose privacy was invaded, only on the intentional interference with the person's seclusion or solitude that would be highly offensive to reasonable persons.[160] The Restatement does not provide guidance on what specific conduct is considered highly offensive to a reasonable person but broadly states that, in order

158. The California court made clear that the inclusion of the requirement that the violating party must intend to invade the occupant's privacy does not require that elements of the invasion of privacy torts be met, merely that the defendant acted to invade the subject's privacy. *In re* M.H., 205 Cal. Rptr. 3d 1, 10 (Ct. App. 2016).

159. RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

160. *Id.* § 652B cmt. a.

for liability to follow, the interference must be a substantial one that occurs as the result of actions to which a reasonable person would object.[161] For example, no liability would result from merely calling the plaintiff on the telephone once or twice in attempts to collect a debt.[162] However, if these phone calls repeatedly occurred with such frequency that they became a burden to the plaintiff's existence, these communications could be seen as invading his privacy.[163]

Given the plethora of news articles reporting that students feel uncomfortable or unnerved by the presence of a remote proctor or proctoring system watching their every move during an online examination, there is support that such conduct is of the sort to which a reasonable person would object.[164] Further, the Supreme Court recognizes that a certain expectation of privacy is present in one's home; this recognition provides further support that to purposefully record a student in their own home would be highly offensive to a reasonable person.[165] Thus, it is possible that students recorded during remote examinations taken from their homes, or other sensitive places, may have a claim that such conduct is highly offensive to a reasonable person and constitutes an intrusion upon seclusion.

B. Data-Protection Remedies

1. Expand FERPA to Address Remote-Proctoring Data-Collection Concerns

FERPA and state biometric-information or privacy laws, in their current versions, do not sufficiently protect students' private biometric information in the modern digital age. However, FERPA can and should be expanded to provide adequate protection for student biometric information nationwide. This Subpart examines the current strengths and shortcomings of FERPA and suggests amending FERPA to provide more comprehensive student-biometric-privacy protection by incorporating portions of state privacy and biometric-information statutes.

161. *Id.* § 652B cmt. d.

162. *Id.*

163. *Id.*

164. *See* Harwell, *supra* note 23; Hubler, *supra* note 9.

165. "At the [Fourth] Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" Florida v. Jardines, 569 U.S. 1, 6 (2013) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

a. FERPA's Strengths

FERPA was adopted to protect student privacy and the confidentiality of student records.[166] As explained in Part II.A.2, FERPA generally prohibits disclosure of personally identifiable information from student educational records without student consent.[167] FERPA includes biometric records within its definition of protected personally identifiable information, meaning any record of a measurable biological or behavioral characteristic that can be used to identify an individual—such as "fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting"—is protected by FERPA.[168] Therefore, FERPA likely already protects the type of biometric data recorded and retained during exam proctoring sessions. Thus, utilizing FERPA as a biometric-privacy law to protect student-test-taker information would not require expanding the Act's definition of personally identifiable information.

Additionally, FERPA is a national statute, applicable to all educational institutions that receive Department of Education funding, including both public and private postsecondary institutions.[169] This existing framework would allow for the broad implementation of biometric-data-privacy protections for students throughout the country, preventing gaps in protection for those who attend private educational institutions.

FERPA's existing framework provides the most convenient vehicle for increasing biometric-data protection for students nationally. However, FERPA in its current form presents several shortcomings that must be addressed to ensure students are adequately protected from the misuse, abuse, or theft of their biometric data.

b. FERPA's Weaknesses

While FERPA aims to protect student privacy and confidentiality, the Act creates no implied private right of action or rights enforceable under 42 U.S.C. § 1983[170] for students whose data or records are misused

166. *See* 34 C.F.R. § 99.2 (2023).

167. *Id.* § 99.30(a).

168. *Id.* § 99.3.

169. *See id.* § 99.1(a)(1)–(2).

170. "Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's

or improperly disclosed by schools or their agents.[171] FERPA's provisions lack "rights-creating" language that signals the congressional intent required to create new rights.[172] Instead the provisions speak only to the Secretary of Education, prohibiting the Department of Education from providing funds to schools or institutions that have policies or practices that violate FERPA's nondisclosure requirements.[173] Rather than allowing students to bring actions against educational institutions or agencies that violate FERPA, Congress authorized the Secretary of Education to handle violations of the Act and required the Secretary to form a board to investigate and adjudicate alleged violations.[174] The Secretary has designated the Office of the Chief Privacy Officer to handle these violations.[175] Students who believe an educational institution has violated FERPA requirements may file a written complaint with that office.[176] If the Office finds that the educational institution or affiliated third party has violated FERPA's provisions, it must notify the institution or third party of the violation and give the organization a reasonable period of time to comply.[177] If an educational institution does not comply, then the Department of Education may withhold further payments, issue a complaint to compel compliance, or terminate eligibility for that institution to receive funding.[178] While these appear to be meaningful consequences for educational institutions that violate FERPA's requirements, the threat of punishment may be just that—a threat; financial penalties have never been assessed against these noncompliant schools.[179]

Further, third-party companies have no true incentive to comply with FERPA's requirements as the U.S. Department of Education does not directly restrict or punish these companies, only the schools that

judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable." 42 U.S.C. § 1983.

171. *See* Gonzaga Univ. v. Doe, 536 U.S. 273, 285–87 (2002) (explaining that "FERPA's nondisclosure provisions fail to confer enforceable rights.").

172. *Id.* at 287 (quoting Alexander v. Sandoval, 532 U.S. 275, 288 (2001)).

173. *Id.*

174. *Id.* at 289; 20 U.S.C. § 1232g(f)–(g).

175. 34 C.F.R. § 99.60 (2023).

176. 34 C.F.R. § 99.63 (2023).

177. 34 C.F.R. § 99.66 (2023).

178. 34 C.F.R. § 99.67(a) (2023).

179. Amy Rhoades, *Big Tech Makes Big Data Out of Your Child: The FERPA Loophole Edtech Exploits to Monetize Student Data*, 9 Am. U. Bus. L. Rev. 445, 451 (2020).

contract with the companies.[180] When personally identifiable information is disclosed to third-party service providers who contracted with educational institutions that qualify as "school officials" under the Act, FERPA still governs its use and the school is still responsible for its protection.[181] However, the companies themselves face no threat of punishment from the Department of Education, and thus are encouraged to follow the requirements by only the terms of the contracts between them and the schools as well as the need for continued business with those schools.[182] To meaningfully regulate behavior of third-party vendors, including remote-proctoring companies, there must be additional penalties or, at the very least, a threat of civil suit for misusing or improperly retaining, selling, or disclosing student data.

Additionally, while FERPA does restrict the disclosure of personally identifiable information from student records without student consent[183] and gives students the right to inspect their records and request that any error in their records be corrected,[184] the Act does not require that educational institutions, or the third parties with which they contract, publish retention schedules notifying students of how long their personal information will be stored.[185] The lack of retention schedules and failure to follow those schedules were at the heart of the previous biometric-data lawsuits filed against remote-proctoring companies and universities by students in Illinois.[186] Inclusion of such retention schedules is vital in fully informing students about the collection and use of their data and is key in minimizing increased security risk of storing data longer than necessary.[187]

180. *See* Susan G. Archambault, *Student Privacy in the Digital Age*, 2021 B.Y.U. EDUC. & L.J. 1, 5.

181. U.S. DEP'T OF EDUC., *supra* note 93, at 2.

182. *See* Brandon Wong, *FERPA: The Joke with No Punchline*, AM. ENTER. INST. (Feb. 23, 2015), https://www.aei.org/education/ferpa-joke-punchline/ [https://perma.cc/JV4F-CM7M]; *see also* 34 C.F.R. § 99.67(c) (2021).

183. 34 C.F.R. §§ 99.30–99.31 (2023).

184. 34 C.F.R. §§ 99.10, 99.20 (2023).

185. However, the Act does require that if an educational institution shares personally identifiable information with third parties to conduct studies on behalf of the school, the information must be destroyed when no longer needed for the study, and the written agreement the school has with the third-party agency must specify the time period in which the information must be destroyed. 34 C.F.R. § 99.31(a)(6)(i), (a)(6)(iii) (2023).

186. *See supra* notes 26–30 and accompanying text.

187. *See supra* note 30 and accompanying text.

2. Recommendations for More Comprehensive Student Biometric Data Protection

To combat the privacy problems caused by remote proctoring technology and provide students with comprehensive protection over the privacy of their biometric data, FERPA should be amended to encompass elements of California's CCPA and STTPPA as well as Illinois's BIPA. The amended Act should utilize the existing FERPA framework but should adopt portions of the California and Illinois privacy laws to fill in the privacy gaps discussed in Part III.B.1.b.[188]

First and foremost, FERPA should be amended to, like the STTPPA, explicitly regulate the activity of companies that contract with educational institutions to provide remote proctoring services and collect student data in the process. By bringing proctoring companies within the group of entities specifically regulated by FERPA, the federal government would have the ability to regulate private companies' behavior directly, rather than indirectly through their agency with schools. This direct regulation may increase private companies' desire to comply with FERPA's disclosure regulations. Additionally, there would be no question of whether the company is truly an agent of the school and could be held to FERPA's requirements.

FERPA should also be amended to emulate the CCPA's and STTPPA's restrictions on proctoring companies' collection, use, retention, and disclosure of personal student data, including biometric data, for only purposes strictly necessary to provide their proctoring services.[189] This would support FERPA's existing purpose of protecting

188. In a 2021 *Brooklyn Law Review* Note, Eliza Simmons discusses problems created by increased collection of biometric data in the private sector, focusing on consumer data-collection, and the need for biometric-privacy regulation. She discusses the existing federal and state privacy laws, including state biometric-privacy laws, and suggests Congress protect consumers' biometric information through federal legislation modeled after the California Consumer Privacy Act. *See* Eliza Simons, *Putting a Finger on Biometric Privacy Laws: How Congress Can Stitch Together the Patchwork of Biometric Privacy Laws in the United States*, 86 BROOK. L. REV. 1097 (2021). This Note, while also discussing a biometric-privacy issue and existing state biometric-privacy laws, focuses narrowly on protecting student biometric information collected during remotely proctored exams by remote-proctoring companies. It suggests that the existing FERPA framework can be amended to incorporate portions of California and Illinois laws to adequately protect student biometric information collected by remote-proctoring companies.

189. *See* CAL. CIV. CODE § 1798.121 (West 2022) (explaining that consumers had the right to request that businesses only use their sensitive personal information for purposes necessary to provide the services requested by

student privacy and confidentiality and would limit the amount of sensitive data collected from students. Further, to allow students to understand if proctoring companies are indeed breaching the new amended requirement to collect, retain, use, and disclose only necessary information, FERPA should be amended to require proctoring companies to disclose to students using their software what information they collect from students, how that information will be used, and whether it will be disclosed or shared, similar to the requirements in the CCPA.[190]

Additionally, as discussed in Parts I.A.2 and III.B.1.b, data retention is a major concern to students and was at the center of student lawsuits against proctoring companies that faced a data breach, compromising thousands of student records, many of which had been retained for over eight years.[191] Illinois's BIPA requires companies that retain biometric information to publish a written retention schedule and guidelines for destroying biometric information once the purpose for collecting the information has been satisfied, and allows for the retention of that data for a maximum of three years since the person the information was collected from last interacted with the business.[192] To protect against the possibility of hackers obtaining improperly retained student biometric information that is no longer necessary for proctoring services, FERPA should be amended to implement a similar retention-publication requirement, and companies and schools should be required to follow those published retention policies.

Finally, like BIPA, FERPA should be amended to contain rights-granting language that gives students a private right of action against proctoring companies or educational institutions that fail to follow either FERPA's existing or this Note's proposed amendments' requirements.[193] Private rights of action are important tools in privacy regulation. They allow each violation of a statute to be the potential

---

the consumer); *see also* CAL. BUS. & PROF. CODE § 22588(a) (West Supp. 2024).

190. *See* CAL. CIV. CODE § 1798.100 (West 2022).

191. *See supra* notes 29–30 and accompanying text.

192. 740 ILL. COMP. STAT. 14/15(a) (2022).

193. The Supreme Court has previously been skeptical of implied private rights of action and scrutinizes statutory language to discern whether Congress intended to create a private right of action. Courts themselves, absent clear congressional intent, cannot create a private right of action, even if desirable as policy matter. *See, e.g.*, Alexander v. Sandoval, 532 U.S. 275, 286–88 (2001). Thus, to ensure individuals can sue educational institutions or proctoring companies that fail to follow FERPA and this Note's amendments, explicit rights-granting language should be added to the statute.

driver of litigation, so private actors can compel companies to comply with the law.[194] Private rights of action allow individuals to pursue claims and seek redress even if public agencies do not have the resources or the desire to do so.[195] "[E]ven if few cases are brought, and fewer are successful, the benefits of a private right of action hold because of their deterrence function. The looming threat of individual action from individual consumers is essential for actually making sure companies are held accountable to privacy laws."[196] Additionally, private rights of action allow individuals the opportunity to enforce their own rights and serve as a recognition of plaintiffs' dignity.[197] This expressive function of private rights of action "increases individuals' belief in their own agency as members of society and rights-bearers."[198] Addressing modern privacy concerns requires a hybrid approach of both public and private enforcement against entities participating in invasive conduct.[199] Amending FERPA to include a private right of action against proctoring companies and educational institutions that improperly collect, use, disclose, or retain students' personally identifiable information, including biometric information, will create a more effective, hybrid enforcement model.

CONCLUSION

The onset of the COVID-19 pandemic led to an increase in online instruction and a corresponding increase in the use of remote proctoring software by universities to help maintain the academic integrity of virtually administered examinations.[200] However, the ubiquity of remote proctoring software use illuminated serious student-privacy concerns. The use of webcams to conduct room scans and forced recordings to peer into the private bedrooms and spaces of students, without their consent, on behalf of public universities, violates the Fourth Amendment's protection against unreasonable searches.[201] Further, while not violative of the Fourth Amendment when conducted on behalf

194. Lauren Henry Scholz, *Private Rights of Action in Privacy Law*, 63 WM. & MARY L. REV. 1639, 1657 (2022).

195. *Id.*

196. *Id.* at 1658.

197. *Id.* at 1663–64.

198. *Id.* at 1666.

199. *Id.* at 1644.

200. *See supra* notes 4–7 and accompanying text.

201. Ogletree v. Cleveland State Univ., 647 F. Supp. 3d 602, 617 (N.D. Ohio 2022), *vacated, appeal dismissed sub nom.* Ogletree v. Bloomberg, No. 22-3795, 2023 WL 8468654 (6th Cir. Dec. 4, 2023).

of a private university, room scans and forced recordings of students in private spaces are invasions of student privacy that should be addressed by state statutes against recording in private spaces. In the absence of such statutes, these invasions of privacy may be redressed by students bringing tort claims of intrusion upon seclusion against schools and proctoring companies.

In addition to unreasonable-search and invasion-of-privacy concerns, students have also raised concerns regarding the collection, use, retention, and disclosure of the personal data that remote-proctoring companies collect during the proctoring process.[202] In 2020, multiple proctoring companies faced security events that put personal student data at risk, prompting Illinois students to file lawsuits against their universities and proctoring companies, alleging that the entities had improperly handled student biometric information.[203] While several states have existing laws aimed at protecting students' sensitive biometric information, each has flaws or gaps, allowing student biometric information to remain vulnerable in the hands of remote-proctoring companies. No national student-biometric-privacy law exists to hold accountable wrongdoing remote-proctoring companies or universities responsible for their misuse of student biometric data. However, FERPA provides a helpful national framework that already aims to protect student privacy.[204] FERPA can and should be amended to incorporate additional provisions from state biometric-data and privacy laws to provide more comprehensive privacy protection for student biometric information. A more comprehensive student-privacy statute is necessary in today's digital age.

While remote proctoring software was largely utilized as a mechanism for allowing remote instruction, and more specifically examination, to continue during the period of isolation and shelter-in-place during the COVID-19 pandemic, it appears likely that such monitoring software is here to stay. However, the security and privacy concerns it carries need not be permanent—action through legislation and judicial proceedings laid out in this Note can prevent the serious invasions of privacy and data-security issues in the future.

Addie Griffey[†]

202. *See supra* notes 24 & 30 and accompanying text.

203. *See supra* notes 26–31 and accompanying text.

204. *See supra* notes 84 & 87 and accompanying text.

† J.D., 2024, Case Western Reserve University School of Law; B.S. Finance, 2019, The Pennsylvania State University. I extend deep thanks to the *Case Western Reserve Law Review* Volume 74 staff for their edits and to Professor Jonathan Entin for his advice and comments on this Note. Additionally, I thank Professor Daniel Jaffe for his suggestion that

partially inspired this Note and Mr. Jeffrey Wolford for encouraging me to pursue a legal career. I would also like to thank my family for their unending love and support throughout law school and Logan for his love and encouragement always.