OFFICE OF THE ATTORNEY GENERAL OF THE DISTRICT OF COLUMBIA
Washington, DC 20001

In the Matter of Online Test Proctoring Companies Respondus, Inc.; ProctorU, Inc.; Proctorio, Inc.; Examity, Inc., and Honorlock, Inc.

Complaint and Request for Investigation, Injunction, and Other Relief

Submitted by

The Electronic Privacy Information Center (EPIC)

I. Summary

1. This complaint concerns five providers of online test proctoring software and services, each of which claims to detect instances of academic dishonesty through the remote monitoring of students during tests and exams. These five firms—Respondus, ProctorU, Proctorio, Examity, and Honorlock (collectively, "Respondents")—use a range of tools to surveil or enable the surveillance of test-takers, including video and audio observation conducted via a test-taker's webcam and microphone; keystroke logging; facial recognition technology; and artificial intelligence ("AI") analysis of the data collected from each student. This complaint specifically addresses Respondents' excessive collection of personal information and use of secret algorithms, which constitute unfair and deceptive trade practices in violation of the D.C. Consumer Protection Procedures Act ("DCCPPA") and the Federal Trade Commission ("FTC") Act. For the reasons set out below, the Office of the Attorney General should open an investigation, enjoin the offending practices, and provide such other relief as EPIC has proposed or the Attorney General finds necessary and appropriate.

II. Parties

2. The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC has played a leading role in developing the authority of state and federal regulators to address emerging privacy issues and to safeguard

the privacy rights of consumers.[1] EPIC is also a longstanding advocate of algorithmic transparency and binding ethical limitations on the use of AI.[2]

3. Respondus, Inc. ("Respondus") is an online test proctoring company with headquarters located at 8201 164th Avenue NE, Suite 200, Redmond, WA 98052.[3] Respondus states that it proctors more online exams in higher education than any other proctoring service and that its technology is "embedded in dozens of third-party learning and assessment platforms."[4] Respondus offers several products for higher education, including LockDown Browser, which temporarily locks down a test-taker's computer during the administration of a test,[5] and Respondus Monitor, which uses AI to analyze recordings obtained via a test-taker's webcam.[6] Respondus's online proctoring technology is used by one or more educational institutions located in the District of Columbia and, on information and belief, is used by test-takers that live and study in the District.

4. ProctorU, Inc. ("ProctorU") is an online test proctoring company with headquarters located at 2200 Riverchase Center, Suite 600, Birmingham, AL 35244.[7] ProctorU states that it proctored 2 million tests last year for more than 750,000 students.[8] ProctorU offers several services to monitor students: Record, an AI-powered exam session tool that produces recordings of test-takers for institutions to review;[9] Record+, which includes the same features as Record but also provides professional proctors to review the recordings;[10] Review+, a "live proctored launch, end-to-end recording solution with artificial intelligence,

---

[1] *See, e.g.*, Complaint of EPIC, *In re Airbnb* (Feb. 26, 2020), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf; Petition of EPIC, *In re Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce* (Feb. 3, 2020), https://epic.org/privacy/ftc/ai/epic-ai-rulemaking-petition/; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf; Comments of EPIC, *In re Unrollme, Inc.,* FTC File No. 172-3139 (Sep. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; Comments of EPIC, *In re Aleksandr Kogan and Alexander Nix*, FTC File Nos. 182-3106 & 182-3107 (Sep. 3, 2019), https://epic.org/apa/comments/EPIC-FTC-CambridgeAnalytica-Sept2019.pdf; EPIC, Comments on Standards for Safeguarding Customer Information (Aug. 1, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint of EPIC, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf; Comments of EPIC, *In re Uber Technologies, Inc.*, FTC File No. 152-3054 (May 14, 2018), https://epic.org/apa/comments/EPIC-FTC-Revised-Uber-Settlement.pdf; Comments of EPIC, *In re Paypal, Inc.* FTC File No. 162-3102, (Mar. 29, 2018), https://epic.org/apa/comments/EPIC-FTC-PayPal-ConsentOrder.pdf.

[2] EPIC, *Algorithmic Transparency: End Secret Profiling* (2019), https://epic.org/algorithmic-transparency/.

[3] *Privacy Contact*, Respondus (2020), https://web.respondus.com/privacy-contact/.

[4] *Who We Are*, Respondus (2020), https://web.respondus.com/.

[5] *LockDown Browser*, Respondus (2020), https://web.respondus.com/he/lockdownbrowser/.

[6] *Respondus Monitor*, Respondus (2020), https://web.respondus.com/he/monitor/.

[7] *Privacy Policy*, ProctorU (2020), https://www.proctoru.com/privacy-policy.

[8] Drew Harwell, *Mass School Closures in the Wake of the Coronavirus are Driving a New Wave of Student Surveillance*, Wash. Post (Apr. 1, 2020), https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/.

[9] *Protect Any Online Exam*, ProctorU (2020), https://www.proctoru.com/.

[10] *Automated Solutions to Deter Proxy Testing, Cheating & Content Theft*, ProctorU (2020), https://www.proctoru.com/services/software-proctoring.

professional review and incident reporting";[11] and Live+, which combines AI with human supervision, "including a live proctored launch, continuous monitoring, active proctor intervention to stop suspicious behavior, comprehensive reporting and more."[12] ProctorU's online proctoring technology is used by one or more educational institutions located in the District of Columbia and, on information and belief, is used by test-takers that live and study in the District.

5. Proctorio, Inc. ("Proctorio") is an online test proctoring company with headquarters located at 6840 E. Indian School Road, Scottsdale, AZ 85251.[13] Proctorio uses a Google Chrome browser extension to collect video, audio, and screen captures and create a recording of a student's exam session.[14] Proctorio also uses AI and facial recognition technology to flag allegedly suspicious behaviors during an exam and delivers an integrity report to the instructor.[15] Proctorio's online proctoring technology is used by one or more educational institutions located in the District of Columbia and, on information and belief, is used by test-takers that live and study in the District.

6. Examity, Inc. ("Examity") is an online test proctoring company with headquarters located at 153 Needham Street, Newton, MA 02464.[16] Examity offers "Automated Proctoring" and "Live Proctoring" services.[17] The company offers two Automated Proctoring options: Automated Standard, which takes an image of a student's official ID, creates a digital "signature" from a student's keystrokes, and produces recording of the exam with time-stamped comments; and Automated Premium, which provides the same services as Automated Standard but also includes a human audit of the authentication, exam, and AI-based findings.[18] Examity offers two Live Proctoring options: Live Standard, which combines the features of Automated Proctoring with human authenticiation and review (plus a required 360° camera sweep of the student's workspace); and Live Premium, which has the same capabilities as Live Standard but includes a live proctor throughout the duration of the exam.[19] Examity's online proctoring technology is used by one or more educational institutions located in the District of Columbia and, on information and belief, is used by test-takers that live and study in the District.

7. Honorlock, Inc. ("Honorlock") is an online test proctoring company with headquarters located at 2500 North Military Trail, Suite 322, Boca Raton, FL 33431.[20] Honorlock uses an in-browser recording and review system through which Honorlock's AI monitors exam sessions, proctors review those sessions, and instructors receive recordings and incident

[11] *Protect Any Online Exam*, *supra* note 9.
[12] *Id.*
[13] *Privacy*, Proctorio (2020), https://proctorio.com/about/privacy.
[14] *Support for Test-Takers*, Proctorio (2020), https://proctorio.com/support.
[15] *Exam Monitoring*, Proctorio (2020), https://proctorio.com/platform/exam-monitoring.
[16] *Contact Us*, Examity (2020), https://www.examity.com/contact-us/.
[17] *Flexible & Easy*, Examity (2020), https://www.examity.com/#.
[18] *Automated Proctoring*, Examity (2020), https://www.examity.com/auto-proctoring/.
[19] *Live Proctoring*, Examity (2020), https://www.examity.com/live-proctoring/.
[20] *Contact*, Honorlock (2020), https://honorlock.com/about-us/.

reports.[21] On information and belief, Honorlock's online proctoring technology is used by test-takers that live and study in the District.

III. Factual Background

8. Although online test proctoring services are not new, the use and reach of such tools has dramatically increased since the beginning of the COVID-19 pandemic as educational institutions have turned to remote learning arrangements.[22]

9. The rapid growth of online test proctoring has all but forced many students to trade away their privacy rights in order to meet their academic obligations. Increasingly, students must submit to invasive audio and video surveillance of their intimate spaces; compulsory collection of biometric and other sensitive personal data; and opaque AI analysis of their movements, facial expressions, and keystrokes.

10. These systems routinely collect sensitive data from students that is not necessary to administer an exam and subject test-takers to secret, unproven algorithms that can effectively accuse them of cheating with no legitimate basis.

11. More than half of educational institutions acknowledge that the violation of student privacy is one of the chief risks associated with online proctoring systems.[23] Yet the use of these tools continues to grow, even as their necessity, efficacy, and reliability remains unproven.[24]

12. According to one survey, the five Respondents represent the most commonly used providers of online proctoring software: Respondus (used by 65% of surveyed educational institutions), ProctorU (23%), Proctorio (17%), Examity (12%), and Honorlock (12%).[25]

13. Online proctoring systems generally fall into one or more of four categories: (1) passive monitoring of software, which tracks applications that are running on student's computer and whether the student switches to a different application during a test; (2) active restriction of software, which uses a "lockdown browser" that blocks access to other applications during an exam; (3) passive video surveillance, which uses software that accesses a student's webcam

[21] *Honorlock*, Honorlock (2020), https://honorlock.com/.
[22] Harwell, *supra* note 8; *see also* Shea Swauger, *Software That Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy*, MIT Technology Review (Aug. 7, 2020), https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/.
[23] Susan Grajek, *Educase COVID-19 QuickPoll Results: Grading and Proctoring*, Educase Review (Apr. 10, 2020), https://er.educause.edu/blogs/2020/4/educause-covid-19-quickpoll-results-grading-and-proctoring.
[24] *See* Bruce Schneier, *The Security Failures of Online Exam Proctoring*, Schneider on Sec. (Nov. 11, 2020), https://www.schneier.com/blog/archives/2020/11/the-security-failures-of-online-exam-proctoring.html ("There are a variety of companies that provide online proctoring services, but they're uniformly mediocre[.]").
[25] *Id.*; *see also id*. at n.1 ("Percentages exceed 100% because most institutions use more than one product.").

and microphone to monitor the student directly; and (4) active video surveillance, which uses passive surveillance software but incorporates live proctors for real-time monitoring.[26]

14. Respondents use a variety of techniques to allegedly establish whether a student "cheats" during an exam. These include requiring each student to upload a picture of their photo ID for authentication;[27] constructing a biometric template of student keystrokes;[28] conducting audio and video surveillance of each student and their surroundings;[29] applying facial recognition;[30] tracking eye movements;[31] and using AI[32] to calculate a "suspicion" score for each student.[33]

15. As a group of U.S. Senators recently noted in their inquiry to a major online test proctoring firm: "Students are not only expected to sit for exams that are being recorded or observed by an unknown virtual proctor, but also install intrusive software and provide extensive personal information—such as images of their home, photos of their identification, and personal information regarding their disabilities. . . . [Q]uestions remain about where and how this data is being used before, during, and after tests, by both your company, the virtual proctors, and testing administrators."[34]

16. Many students have protested the use of online proctoring systems and the "aggressive tactics employed by proctoring companies in response to those efforts."[35] Some educators, including faculty at the University of California at Santa Barbara, have also advised against the use of test proctoring services in remote learning.[36]

17. Students and educators have similarly objected to the risk of unfair and discriminatory treatment by online proctoring systems, warning that opaque algorithms can encode bias and disproportionately harm students of color, students with disabilities, low-income students, and students with children.[37]

---

[26] Grajek, *supra* note 23.
[27] Jason Kelley & Lindsay Oliver, *Proctoring Apps Subject Students to Unnecessary Surveillance*, Elec. Frontier Found. (Aug. 20, 2020), https://www.eff.org/deeplinks/2020/08/proctoring-apps-subject-students-unnecessary-surveillance.
[28] *Id.*
[29] Harwell, *supra* note 8.
[30] Kelley & Oliver, *supra* note 27.
[31] Harwell, *supra* note 8.
[32] *Id.*
[33] *Id.*
[34] Letter from Sen. Richard Blumenthal et al. to Sabastian, Chief Exec. Officer, ExamSoft, at 2 (Dec. 3, 2020), https://www.blumenthal.senate.gov/imo/media/doc/2020.12.3%20Letter%20to%20Ed%20Testing%20Software%20Companies%20ExamSoft.pdf.
[35] Todd Feathers & Janus Rose, *Students Are Rebelling Against Eye-Tracking Exam Surveillance Tools*, Vice (Sep. 24, 2020), https://www.vice.com/en/article/n7wxvd/students-are-rebelling-against-eye-tracking-exam-surveillance-tools.
[36] Madeline Thompson, *UCSB Faculty Association Issues Letter Advising Against the Use of ProctorU Testing Services*, Daily Nexus (Mar. 16, 2020), https://dailynexus.com/2020-03-16/ucsb-faculty-association-issues-letter-advising-against-the-use-of-proctoru-testing-services/.
[37] Feathers & Rose, *supra* note 35.

18. As the same Senators wrote: "[S]tudents have run head on into the shortcomings of these technologies—shortcomings that fall heavily on vulnerable communities and perpetuate discriminatory biases. . . . We are concerned that the software has not been designed to be inclusive and mindful of all students' needs and proctors are not getting the training or information they need to adequately work with and oversee students taking the exams."[38]

19. Respondents have provided little detail about the logic of the algorithms they deploy to flag instances of alleged academic dishonesty or the precise ways in which companies use test-takers' biometric and other personal information.

A. Respondents' Excessive Collection of Personal Data

20. Respondents' collection of sensitive personal information, including biometric data, is unjustified, excessive, and harmful to students who have no meaningful opportunity to opt out of such systems.

21. Online proctoring systems need not falsely flag a student in order to cause real harm. Forcibly collecting personal information from test-takers, including sensitive biometric data, is inherently invasive. Such collection deprives students of control over their personal data;[39] can reveal intimate details about a student's physical features, behaviors, disabilities, family members, and home; and can induce undue stress on test-takers that undermines the integrity of exam sessions—the very thing that test proctoring systems are ostensibly meant to guard against.[40]

22. Respondents have failed to establish the need for the systematic collection of biometric and other personal data from test-takers. The level of individualized surveillance students face from remote proctoring systems far exceeds what they would face in a classroom or take-home test setting. Indeed, many colleges and universities had successfully administered take-home and self-proctored exams for years before Respondents introduced surveillance-based test proctoring systems. Notably, some research even suggests that students taking online courses are *less* likely to cheat than students taking live courses—not more.[41]

---

[38] Blumenthal et al., *supra* note 34, at 2.
[39] *See* Anita L. Allen, *The Wanted Gaze: Accountability for Interpersonal Conduct at Work*, 89 Geo. L.J. 2013, 2017 (2001) ("Privacy in America can be destroyed by failures to guard against 'unwanted gazes.'").
[40] *See* Anushka Patil & Jonah Engel Bromwich, *How It Feels When Software Watches You Take Tests*, N.Y. Times (Sep. 29, 2020), https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html.
[41] George Watson & James Sottile, *Cheating in the Digital Age: Do Students Cheat More in Online Courses?*, Online J. Distance Learning Admin., Spring 2010, https://www.westga.edu/~distance/ojdla/spring131/watson131.html ("The focus of this study was on whether students cheat more in on-line or live courses, and, somewhat surprisingly, the results showed higher rates of academic dishonesty in live courses.").

Respondus

23. Respondus offers several products to academic institutions. One product, Respondus Monitor, "enables students to record themselves with a webcam and microphone during an online exam."[42] Respondus Monitor processes the recordings automatically.[43]

24. Respondus Monitor uses AI that analyzes facial imagery, motions, lighting, keyboard activity, mouse movements, hardware changes, and comparisons to other students who took the exam.[44] At the beginning of a proctoring session, a student may also be forced to show identification to the camera or make a video of the student's surroundings.[45]

25. A student enrolled at an institution which uses Respondus Monitor cannot reasonably avoid Respondus's invasive collection of biometric and personal information or its video surveillance of the student's intimate surroundings.

26. Repondus has failed to identify benefits to consumers or competition that would outweigh the significant privacy harms suffered by students who are subjected to its compulsory collection of personal data.

27. Respondus has also made misleading statements for which it lacks a reasonable basis concerning its sharing of the personal information it collects from students.

28. Although Respondus states that "[o]nly users with instructor credentials for [a] course . . . are able to view video sessions in conjunction with the student identifiable information," Respondus admits that "[r]andom samples of video and/or audio recordings" "may be shared with researchers (research institutions and/or biometric experts) under contract with Respondus,"[46] a transfer of data which would necessarily include identifiable images of students' faces.

ProctorU

29. ProctorU requires each student to provide camera access, microphone access, screen access, and a photo ID to begin an exam.[47] ProctorU uses facial recognition software and biometric keystroke measurements to authenticate a student's identity.[48] ProctorU monitors a student's screen, camera, and microphone continually during an exam.[49]

---

[42] *Additional Privacy Information – Respondus Monitor*, Respondus (2020), https://web.respondus.com/privacy/privacy-additional-monitor/.
[43] *Id.*
[44] *Respondus Monitor*, *supra* note 6 (click "Monitor AI").
[45] *Id.* (click "A fully automated solution").
[46] *Terms of Use - Respondus Monitor (Institution)*, Respondus (2020), https://web.respondus.com/tou-monitor-admin/.
[47] *Privacy Policy*, *supra* note 7.
[48] *Id.*
[49] *Id.*

30. A student enrolled at an institution which use's ProctorU's online proctoring system cannot reasonably avoid ProctorU's invasive collection of biometric and other personal information or its video surveillance of the student's intimate surroundings.

31. ProctorU has failed to identify benefits to consumers or competition that would outweigh the significant privacy harms suffered by students who are subjected to its compulsory collection of personal data.

32. ProctorU has also made misleading statements for which it lacks a reasonable basis concerning its collection of personal information.

33. ProctorU represents that "ProctorU does not use any test-taker's personal information for any purpose other than for facilitating the proctoring of online exams."[50] Yet according to CEO Scott McFarland, ProctorU maintains a "Hall of Fame" video composed of alleged instances of cheating.[51] Such a video, although clearly unnecessary "for facilitating the proctoring of online exams," would necessarily include identifiable images of students.

34. Recently, the Faculty Association at the University of California at Santa Barbara criticized ProctorU for its inadequate privacy policy and related privacy concerns.[52] As the Association explained: "[O]ne can see the categories of information that ProctorU regularly collects and discloses to third parties which include: social security numbers; driver's license and passport numbers; other personal identifiers and biometric information including genetic, physiological, behavioral, gender identity, and biological characteristics; activity patterns and identifying information unique to each user including fingerprints, faceprints, voiceprints, iris or retina scans; IP addresses or device identifiers; browsing history, search history, and information about students' interactions with websites, applications, or advertisements; medical information including medical conditions, physical disability, and/or mental disability; photographs, video, and audio recordings; education and employment information including that related to citizenship."[53] ProctorU has since updated its privacy policy.

Proctorio

35. Proctorio's online proctoring system records video and audio of students during an exam if the instructor so chooses.[54] In at least some cases, Proctorio can "[r]ead and change all [of the] data on the websites [a student] visits" during an exam.[55]

---

[50] *Id.*
[51] Harwell, *supra* note 8.
[52] Paul Levy, *Can ProctorU Be Trusted With Students' Personal Data?*, Pub. Citizen (Mar. 25, 2020), https://pubcit.typepad.com/clpblog/2020/03/can-proctoru-be-trusted-with-students-personal-data.html.
[53] Letter from UC Santa Barbara Fac. Assoc. to Chancellor Henry T. Yang & Exec. Vice Chancellor David Marshall, Univ. of Cal., Santa Barbara (Mar. 13, 2020), https://cucfa.org/wp-content/uploads/2020/03/ProctorU_2020-1.pdf.
[54] *Privacy*, *supra* note 13.
[55] *Id.*

36. Proctorio requires students to agree to monitoring "by webcam, microphone, browser, desktop, or any other means necessary to uphold integrity."[56] Proctorio tracks speech, eye movements, mouse clicks, and how long each student took to complete an exam in order to calculate a "suspicion level" for the student.[57]

37. Proctorio's dissemination of personally identifiable information has recently come under fire. After a Reddit user complained that Proctorio's support staff was unhelpful when the software crashed during his midterm exam,[58] Proctorio CEO Mike Olsen posted a copy of the student's chat logs with the support staff and wrote, "If you're gonna lie bro . . . don't do it when the company clearly has an entire transcript of your conversation."[59] This response was "quickly panned as an inappropriate use of corporate data and an invasion of privacy. Olsen apologized and removed the chat logs."[60]

38. A student enrolled at an institution which uses Proctorio's online proctoring system cannot reasonably avoid Proctorio's invasive collection of personal information or its video surveillance of the student's intimate surroundings.

39. Proctorio has failed to identify benefits to consumers or competition that would outweigh the significant privacy harms suffered by students who are subjected to its compulsory collection of personal data.

Examity

40. Examity views and records each student's webcam feed and computer screen during the the course of an exam.[61] Examity also states that it "may collect" a "biometric record," defined as "a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, such as fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting."[62]

41. A student enrolled at an institution which uses Examity's online proctoring system cannot reasonably avoid Examity's invasive collection of biometric and other personal information or its video surveillance of the student's intimate surroundings.

42. Examity has failed to identify benefits to consumers or competition that would outweigh the significant privacy injuries suffered by students who are subjected to its compulsory collection of personal data.

---

[56] Harwell, *supra* note 8.
[57] *Id.*
[58] Todd Feathers, *An Exam Surveillance Company Is Trying to Silence Critics with Lawsuits*, Vice (Oct. 21, 2020), https://www.vice.com/en/article/7k9zjy/an-exam-surveillance-company-is-trying-to-silence-critics-with-lawsuits.
[59] *Id.*
[60] *Id.*
[61] *Product Privacy Policy*, Examity (2020), https://www.examity.com/product-privacy-policy/.
[62] *Id.*

Honorlock

43. Honorlock uses a Google Chrome browser extension to collect video and audio recordings of test-takers, to monitor desktop activity, and to track webpages visited by each student during an exam.[63]

44. A student enrolled at an institution which uses Honorlock's online proctoring system cannot reasonably avoid Honorlock's invasive collection of biometric and other personal information or its video surveillance of the student's intimate surroundings.

45. Honorlock has failed to identify benefits to consumers or competition that would outweigh the significant privacy injuries suffered by students who are subjected to its compulsory collection of personal data.

B. Respondents' Use of Opaque AI and Secret Algorithms

46. The use of artificial intelligence—and particularly the use of an AI system that can impose tangible, adverse consequences on individuals—must adhere to rigorous ethical and human rights standards.

47. The Organisation for Economic Co-operation and Development ("OECD") Principles on Artificial Intelligence make clear that an entity deploying an AI system must respect "freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, [and] fairness"; that the entity must be "accountable for the proper functioning of [the] AI system[]"; and that the entity must exercise "transparency and responsible disclosure," including "easy-to-understand information on the factors, and the logic that served as the basis for [any] prediction, recommendation or decision" by the AI system.[64]

48. Respondents' use of AI to remotely monitor students and identify purported instances of cheating fails to satisfy these basic principles of privacy, fairness, non-discrimination, accountability, and transparency.

49. Respondents routinely subject students to extensive collection of biometric and other sensitive personal information; deploy opaque and unproven AI tools to process that data; and fail to fully disclose to students the logic, factors, and determinations of the AI systems that claim to detect and flag signs of cheating.

[63] *Honorlock Protects Student Privacy*, Honorlock (2020), https://honorlock.com/studentprivacy/.
[64] *Recommendation of the Council on Artificial Intelligence*, OECD (May 21, 2019) [*hereinafter OECD AI Principles*], legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

50. Although these AI-based flags may "harm [student]s' life opportunities often in arbitrary and discriminatory ways,"[65] students typically do not have access to the flags raised during an exam session or know of the precise logic behind a flag. [66]

51. Respondents market their services as a way to eliminate bias and promote efficiency during the online exam proctoring process. But AI tools frequently introduce or exacerbate bias rather than eliminate it.[67]

52. For example, facial recognition systems have repeatedly been found less effective at identifying or evaluating faces of color. A 2017 study of facial recognition systems found that darker-skinned females were 32 times more likely to be misclassified than lighter-skinned males.[68] Facial recognition systems may also analyze emotions differently based on the individual's race.[69] A 2018 analysis found that facial recognition system Face++ "consistently interpret[ed] black [basketball] players as angrier than white players, even controlling for their degree of smiling," while Microsoft AI "interpret[ed] black players as more contemptuous when their facial expression [was] ambiguous."[70]

53. AI tools often exhibit gender bias, as well. In 2018, Amazon abandoned an AI recruiting tool because the system determined from historical employee data that male candidates were preferable. The system penalized resumes that included the word "women's" and the names of all-women's colleges.[71] The two factors the system found most indicative of strong job performance were if the applicant's name was Jared and if the applicant played high school lacrosse.[72]

54. AI systems that detect movements or rely on eye tracking are prone to inaccurately flagging students with disabilities and neurological differences.[73] As disability justice advocate Lydia X. Z. Brown recently explained, "The point [of these systems] is to identify and flag atypical movement, behavior, or communication; disabled people are by definition going to move,

---

[65] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 7–8 (2014).
[66] *See, e.g.*, *Flag System*, Examity (2020), https://www.examity.com/flag-system/.
[67] *See, e.g.*, Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, Harv. Bus. Rev. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.
[68] Joy Buolamwini*, Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*, MIT Media Lab (Aug. 10, 2017), https://www.media.mit.edu/publications/full-gender-shades-thesis-17/.
[69] *See generally* Lauren Rhue, Racial Influence on Automated Perceptions of Emotions (2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.
[70] *Id.*
[71] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters (Oct. 9, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.
[72] Dave Gershgorn, *Companies Are on the Hook if Their Hiring Algorithms Are Biased*, Quartz (Oct. 22, 2018), https://qz.com/1427621/companies-are-on-the-hook-if-their-hiring-algorithms-are-biased/.
[73] Shea Swauger, *Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education*, Hybrid Pedagogy (Apr. 2, 2020), https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/.

behave, and communicate in atypical ways."[74] For example, one student who has a chronic tic disorder had to provide her institution with medical records because she feared her involuntary mouth movements would be flagged as cheating.[75] The student reported that her professors having access to footage of her facial tic felt like an invasion of privacy.[76]

55. Similarly, keystroke-analysis—which measures typing speeds, rhythms, and patterns and flags inconsistent typing as a possible sign of cheating—often cannot accurately identify students who have certain medical conditions or physical disabilities that affect their typing.[77]

56. Test-takers who have been harmed by unfair, opaque AI proctoring systems include a student who was falsely flagged for cheating and given a zero simply because she was reading a question aloud;[78] a student who was forced to urinate during an exam to maintain eye contact with her camera;[79] a student of color who was forced to stand on a table to find sufficient light for the software to detect her;[80] and a Muslim woman who was forced to defer an exam because the proctoring system could not properly identify her while she wore a hijab.[81]

Respondus

57. Respondus markets its AI-powered test proctoring system to educational institutions as a tool to prevent cheating and maintain exam integrity.[82]

58. Respondus claims to use an "elegant, functional, powerful" method to rank proctoring results according to the risk that exam violations have occurred,[83] yet the company "disclaims

[74] 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/.
[75] Patil & Bromwich, *supra* note 40.
[76] *Id.*
[77] Shea Swauger, *Remote Testing Monitored by AI Is Failing the Students Forced to Undergo It*, NBC News (Nov. 2020), https://www.nbcnews.com/think/opinion/remote-testing-monitored-ai-failing-students-forced-undergo-it-ncna1246769.
[78] Margot Harris, *A Student Says Test Proctoring AI Flagged Her as Cheating When She Read a Question out Loud. Others Say the Software Could Have More Dire Consequences*, Insider (Oct. 4, 2020), https://www.insider.com/viral-tiktok-student-fails-exam-after-ai-software-flags-cheating-2020-10.
[79] Drew Harwell, *Cheating-Detection Companies Made Millions During The Pandemic. Now Students Are Fighting Back*, Wash. Post (Nov. 12, 2020), https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/.
[80] Patil & Bromwich, *supra* note 40.
[81] Aishah Hussain, *BPTC Student 'Forced to Defer' Exams Over Fears She'd Have to Remove Headscarf for Male Invigilator*, Legal Cheek (Aug. 14, 2020), https://www.legalcheek.com/2020/08/bptc-student-forced-to-defer-exams-over-fears-shed-have-to-remove-headscarf-for-male-invigilator/.
[82] *Who We Are*, Respondus, *supra* note 4.
[83] *Respondus Monitor*, *supra* note 6 (click "Review Priority").

responsibility or liability for the accuracy, content, completeness, legality, reliability, operability or availability of information or data in Respondus Monitor."[84]

59. The AI used in Respondus Monitor has several components.[85] First, the AI applies "advanced algorithms" to detect faces, motion, and lighting changes. Next, the AI analyzes keyboard activity, mouse movements, hardware changes, and other computer device data to identify patterns and outliers associated with cheating. Finally, the AI analyzes each student's exam interactions, including a question-by-question analysis to compare against other students who took the same exam.[86]

60. According to Respondus, Respondus Monitor provides instructors with "simple, meaningful results that help them know whether an exam session warrants deeper scrutiny."[87] Instructors may view the data that contributes to a student's review priority on a video timeline, "such as flagged events and key milestones."[88]

61. Although Respondus uses AI to analyze extensive personal data collected from students, and although that analysis may lead to a student's exam being flagged for signs of cheating and ultimately rejected, Respondus has failed to fully disclose to students the logic, factors, and determinations of its AI.

62. A student enrolled at an institution which uses Respondus Monitor cannot reasonably avoid the determinations of Respondus's opaque, unproven, and potentially biased AI.

63. Repondus has failed to identify benefits to consumers or competition that would outweigh the harms suffered by students who are subjected to its opaque, unproven, and potentially biased AI.

ProctorU

64. ProctorU offers several services to educational institutions to monitor students during exams. Review+ and Live+ both use AI to flag certain behavior such as lighting changes and unusual noises.[89] For example, ProctorU uses AI to recognize low audible voices, slight lighting variations, and "other behavioral cues."[90] The AI time-stamps any flagged events in the recording of the student's exam.[91]

65. Although ProctorU uses AI to analyze extensive personal data collected from students, and although that analysis may lead to a student's exam being flagged for signs of cheating and

[84] *Terms of Use - Respondus Monitor (Student)*, Respondus (2020), https://web.respondus.com/tou-monitor-student/.
[85] *Id.*
[86] *Respondus Monitor*, *supra* note 6 (click "Monitor AI" tab).
[87] *Id.* (click "Review Priority").
[88] *Id.*
[89] *Live+*, ProctorU (2020), https://www.proctoru.com/services/live-online-proctoring.
[90] *FAQ*, ProctorU (2020), https://www.proctoru.com/faq.
[91] *Id.*

ultimately rejected, ProctorU has failed to fully disclose to students the logic, factors, and determinations of its AI.

66. A student enrolled at an institution which uses ProctorU's exam monitoring system cannot reasonably avoid the determinations of ProctorU's opaque, unproven, and potentially biased AI.

67. ProctorU has failed to identify benefits to consumers or competition that would outweigh the harms suffered by students who are subjected to its opaque, unproven, and potentially biased AI.

Proctorio

68. Proctorio's test proctoring system works by recording students, their audio, and their screens to generate "automated suspicion report[s]."[92] Each report includes a "suspicion level" based on the student's behavior during an exam. "The suspicion level is a quick calculation based on the aggregation of frames during the exam which were deemed suspicious and the detection of abnormal behavior."[93]

69. Proctorio uses a "completely software-driven approach."[94] Proctorio's service includes "ID verification, automated proctoring, content protection, secure browser settings, computer lock down, originality authentication, administrative and faculty controls, and deep, instantaneous analytics."[95]

70. Proctorio claims, without proof, that its software "eliminates human error [and] bias[.]"[96]

71. Proctorio recently came under scrutiny when learning technology specialist Ian Linkletter tweeted a critical analysis of the platform.[97] Linkletter explained that Proctorio's system was invasive of students' privacy and alleged that it discriminates against students who are marginalized, neurodiverse, or who otherwise do not fit the developers' definition of normal.[98] In response, Proctorio filed suit against Linkletter in the Supreme Court of British Columbia for sharing what it described as confidential information.[99]

72. Although Proctorio uses AI to analyze extensive personal data collected from students, and although that analysis may lead to a student's exam being flagged for signs of cheating and

[92] Laszlo Richard Toth, *Students Raise Concerns Over Virtual Proctoring*, Daily Illini (Apr. 17, 2020), https://dailyillini.com/news/2020/04/17/proctorio-concerns/.
[93] Proctorio, *Proctorio Gradebook in Canvas* 3 (2020), http://www.fullerton.edu/it/services/software/proctorio/Canvas%20Proctorio%20Gradebook.pdf.
[94] Harwell, *supra* note 8.
[95] *Platform*, Proctorio (2020), https://proctorio.com/platform.
[96] Proctorio (2020), https://proctorio.com/.
[97] Feathers, *supra* note 58.
[98] *Id.*
[99] *Id.*

ultimately rejected, Proctorio has failed to fully disclose to students the logic, factors, and determinations of its AI.

73. A student enrolled at an institution which uses Proctorio's exam monitoring system cannot reasonably avoid the determinations of Proctorio's opaque, unproven, and potentially biased AI.

74. Proctorio has failed to identify benefits to consumers or competition that would outweigh the harms suffered by students who are subjected to its opaque, unproven, and potentially biased AI.

Examity

75. Examity uses AI in its "flag system," which applies time-stamped flags to the recording of a student's exam session to alert the instructor of potential integrity issues.[100]

76. During the authentication process, Examity flags behaviors such as when a "student's typing rhythm differs slightly from when they filled out their profile" or when a student does not type the correct answer to a challenge question on the first try.[101]

77. Test-takers are not made aware of when they are flagged during the exam session.[102] Examity does not notify test-takers of their flags, and test-takers are unable to view their flags or flagging history.[103]

78. Although Examity uses AI to analyze extensive personal data collected from students, and although that analysis may lead to a student's exam being flagged for signs of cheating and ultimately rejected, Examity has failed to fully disclose to students the logic, factors, and determinations of its AI.

79. A student enrolled at an institution which uses Examity's exam monitoring system cannot reasonably avoid the determinations of Examity's opaque, unproven, and potentially biased AI.

80. Examity has failed to identify benefits to consumers or competition that would outweigh the harms suffered by students who are subjected to its opaque, unproven, and potentially biased AI.

Honorlock

81. Honorlock uses a combination of AI proctoring and live proctoring during exams. While taking an exam, Honorlock's AI monitors a student and will trigger a live proctor to drop in

[100] *Flag System*, *supra* note 66.
[101] *Id.*
[102] *Id.*
[103] *Id.*

on the student's feed if the AI "senses that something is wrong."[104] For example, Honorlock's AI will trigger a live proctor when a student diverts their eyes from the screen or gets up from their desk.[105]

82. Although Honorlock uses AI to analyze extensive personal data collected from students, and although that analysis may lead to a student's exam being flagged for signs of cheating and ultimately rejected, Honorlock has failed to fully disclose to students the logic, factors, and determinations of its AI.

83. A student enrolled at an institution which uses Honorlock's exam monitoring system cannot reasonably avoid the determinations of Honorlock's opaque, unproven, and potentially biased AI.

84. Honorlock has failed to identify benefits to consumers or competition that would outweigh the harms suffered by students who are subjected to its opaque, unproven, and potentially biased AI.

IV. Legal Background

A. The D.C. Consumer Protection Procedures Act and Federal Trade Commission Act

85. The D.C. Consumer Protection Procedures Act prohibits unfair and deceptive acts and practices[106] and empowers the Attorney General for the District of Columbia to enforce the Act's prohibitions.[107]

86. The DCCPPA prohibits misrepresentations "as to a material fact which has a tendency to mislead"[108] and failures "to state a material fact if such failure tends to mislead[.]"[109]

87. The DCCPPA provides that "[i] n construing the term 'unfair or deceptive trade practice' due consideration and weight shall be given to the interpretation by the Federal Trade Commission and the federal courts of the term 'unfair or deceptive act or practice'" as employed in Section 5 of the FTC Act, 15 U.S.C. § 45.[110]

88. Section 5 of the FTC Act, like the DCCPPA, prohibits unfair and deceptive acts and practices.[111]

[104] *Frequently Asked Questions*, Honorlock (2020), https://honorlock.com/students/#faq.
[105] *Id.*
[106] D.C. Code § 28-3904.
[107] D.C. Code § 28-3909.01.
[108] D.C. Code § 28-3904(e).
[109] D.C. Code § 28-3904(f).
[110] D.C. Code § 28-3901(d).
[111] 15 U.S.C. § 45(a)(1).

89. Under the FTC Act, a company engages in a deceptive trade practice if it makes a representation to consumers yet "lacks a 'reasonable basis' to support the claims made[.]"[112]

90. A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[113]

91. In determining whether a trade practice is unfair under the FTC Act, regulators are expected to consider "established public policies."[114]

92. The OECD Principles on Artificial Intelligence and the Universal Guidelines for Artificial Intelligence are "established public policies" within the meaning of the FTC Act.[115]

B. The OECD Principles on Artificial Intelligence

93. The Organization for Economic Cooperation and Development ("OECD") was established in 1961 to promote economic cooperation and development.[116] There are presently 36 members of the OECD, including the United States.[117]

94. In 2019, the member nations of the OECD, working with many non-OECD members countries, promulgated the OECD Principles on Artificial Intelligence.[118]

95. The United States has endorsed the OECD AI Principles.[119]

96. Under the OECD AI Principle on Human-Centered Values and Fairness, "AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity, and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognized labour rights."[120]

97. Under the OECD AI Principle on Robustness, Security, and Safety, "AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use,

---

[112] *Daniel Chapter One v. FTC*, 405 F. App'x 505, 506 (D.C. Cir. 2010) (quoting *Thompson Med. Co., Inc. v. FTC*, 791 F.2d 189, 193 (D.C. Cir. 1986)).
[113] 15 U.S.C. § 45(n); *see also FTC v. Seismic Entm't Prods., Inc.*, Civ. No.1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").
[114] 15 U.S.C. § 45(n).
[115] *Id.*; *see also* Petition of EPIC, *supra* note 1.
[116] *History*, OECD, oecd.org/about/history.
[117] *Id.*
[118] *OECD AI Principles*, *supra* note 64.
[119] Fiona Alexander, *U.S. Joins with OECD in Adopting Global AI Principles*, NTIA Blog (May 22, 2019), https://www.ntia.gov/blog/2019/us-joins-oecd-adopting-global-ai-principles.
[120] *OECD AI Principles*, *supra* note 64.

foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk."[121]

98. Under the OECD AI Principle on Transparency and Explainability, AI Actors should "provide meaningful information, appropriate to the context, and consistent with the state of art (i) to foster a general understanding of AI systems, (ii) to make stakeholders aware of their interactions with AI systems, including in the workplace, (iii) to enable those affected by an AI system to understand the outcome, and (iv) to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."[122]

99. Under the OECD AI Principle on Accountability, "[o]rganisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles."[123]

C. The Universal Guidelines for Artificial Intelligence

100. The Universal Guidelines for Artificial Intelligence ("UGAI"), a framework for AI governance based on the protection of human rights, were set out at the 2018 meeting of the International Conference on Data Protection and Privacy Commissioners in Brussels, Belgium.[124]

101. The UGAI have been endorsed by more than 290 experts and 60 organizations in 40 countries.[125]

102. Under the UGAI Right to Transparency, "All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome."[126]

103. Under the UGAI Assessment and Accountability Obligation, "An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks."[127]

104. Under the UGAI Accuracy, Reliability, and Validity Obligations, "Institutions must ensure the accuracy, reliability, and validity of decisions."[128]

---

[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Universal Guidelines for Artificial Intelligence*, The Public Voice (Oct. 23, 2018) [Hereinafter *UGAI*], https://thepublicvoice.org/ai-universal-guidelines/.
[125] *Universal Guidelines for Artificial Intelligence: Endorsement*, The Public Voice (Oct. 23, 2019), https://thepublicvoice.org/AI-universal-guidelines/endorsement/.
[126] *UGAI*, *supra* note 124.
[127] *Id.*
[128] *Id.*

105. Under the UGAI Fairness Obligation, "Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions."[129]

V. Legal Analysis

A. Respondents' Unfair and Deceptive Collection of Excessive Personal Data

106. As set forth above, Respondents collect extensive personally identifiable information, including biometric data, in the course of monitoring students' exam sessions.

107. Respondents variously represent that they protect students' privacy and collect only as much personal data as required to provide their services.[130]

108. But in view of the excessive and intimate personal data that Respondents collect from students—and the harms that such collection causes—Respondents lack a reasonable basis to support these claims.

109. Respondents' collection of personal information unnecessarily deprives students of control over their data; can reveal sensitive details about a student's physical features, behaviors, disabilities, family members, and home; and can induce undue stress in test-takers that undermines the integrity of their exam sessions.

110. Moreover, a student enrolled at an institution which uses one or more of Respondents' online proctoring systems cannot reasonably avoid the collection of biometric and other personal information or video surveillance of their intimate surroundings.

111. Respondents have also failed to identify benefits to consumers or competition that would outweigh the significant privacy injuries suffered by students subject to compulsory data collection. Educational institutions have long shown that they can administer remote and take-home exams without relying on in-home surveillance systems. Respondents have not demonstrated why such surveillance is necessary now or established any benefit from these systems that could outweigh the harms to test takers.

112. Respondents have therefore engaged in unfair and deceptive trade practices in violation of D.C. Code §§ 28-3904, 28-3904(e), and 28-3904(f) and 15 U.S.C. § 45(a)(1).

---

[129] *Id.*

[130] *Respondus Privacy Policy*, Respondus (2020), https://web.respondus.com/privacy-policy/; *Privacy Policy*, *supra* note 7; *Privacy by Design*, Proctorio (2020), https://proctorio.com/about/privacy; *Product Privacy Policy*, *supra* note 61; *Student Privacy Statement,* Honorlock (2020), https://honorlock.com/student-privacy-statement/.

B. Respondents' Unfair Use of Opaque, Unproven AI Systems

i. Respondents' AI-Based Assessments are Unfair Under the DCCPPA and the FTC Act

113. As set forth above, Respondents use biometric and other personal data, opaque AI, and secret algorithms to assess whether a student allegedly engaged in academic dishonesty during an exam.

114. Although Respondents' AI systems may flag students' exams for signs of cheating and ultimately lead to their rejection, Respondents have failed to fully disclose to students the logic, factors, and determinations of those AI systems. This makes it impossible for test-takers to know how their personal data is being used or to meaningfully consent to such uses.

115. In addition to the potential academic consequences of Respondents' AI determinations, Respondents' secret analysis of biometric data and other personal data causes substantial privacy harms to test-takers.

116. Moreover, Respondents' use of biometric data and secret algorithms causes or is likely to cause substantial injury to a large class of people: namely, the millions of students[131] taking tests and exams required by their academic institutions.

117. A student enrolled at an institution which uses one or more of Respondents' online proctoring systems cannot opt out of or otherwise reasonably avoid Respondents' opaque, unproven, and potentially biased AI systems.

118. Respondents have also failed to identify benefits to consumers or competition that would outweigh the significant privacy injuries suffered by students who are subject to AI determinations.

119. Respondents' uses of AI are "unfair" because they "caus[e] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[132]

120. Respondents have therefore engaged in an unfair trade practice in violation of D.C. Code § 28-3904 and 15 U.S.C. § 45(a)(1).

ii. Respondents' AI-Based Assessments Violate the OECD AI Principles

121. Respondents' AI-based assessments of test-takers are not transparent.

122. Test-takers are prevented from fully evaluating or knowing the basis for Respondents' AI-based assessments.

[131] Harwell, *supra* note 8.
[132] 15 U.S.C. § 45(n).

123. As a result, Respondents cannot be held accountable by students for the proper functioning of their AI-based assessments.

124. Respondents have therefore violated the OECD Principles on Artificial Intelligence, an "established public polic[y]" framework within the meaning of the FTC Act.[133]

iii. Respondents' AI-Based Assessments Violate the Universal Guidelines for AI

125. Respondents do not provide test-takers with full access to the factors, logic, and techniques used to generate each AI-based assessment.

126. Respondents have not adequately evaluated whether the purpose, objectives, and benefits of their AI-based assessments outweigh the risks.

127. Respondents have not adequately demonstrated the accuracy of their AI-based assessments.

128. Respondents have not adequately demonstrated the reliability of their AI-based assessments.

129. Respondents have not adequately demonstrated the validity of their AI-based assessments.

130. Respondents have not adequately established that their AI-based assessments are free of unfair bias and impermissible discrimination.

131. Respondents have therefore violated the Universal Guidelines for Artificial Intelligence, an "established public polic[y]" framework within the meaning of the FTC Act.[134]

C. Proctorio and Honorlock's Deceptive Uses of Facial Recognition Tools

132. Respondents Proctorio and Honorlock represent that their proctoring systems do not employ facial recognition.[135] In fact, both companies use tools that meet the FTC's definition of facial recognition.

133. Proctorio contends that, rather than using facial recognition, it employs "facial detection," which "is used to see if a test taker is looking away from the screen for an extended period of time, if there are other people present in the test-taking environment, or if the test taker has left the exam for any reason,"[136] Proctorio also states that it uses "gaze detection,"[137] which "can identify where a person is looking but cannot identify what they are looking at."[138]

---

[133] *Id.*
[134] *Id.*
[135] *See Frequently Asked Questions*, Proctorio (2020), https://proctorio.com/frequently-asked-questions; *Student Privacy FAQ*, Honorlock (2020), https://honorlock.com/studentprivacy/#faq.
[136] *Frequently Asked Questions, supra* note 135.
[137] *Why Proctorio Does Not Use Facial Recognition*, ProctorioBlog (Aug. 16, 2020), https://blog.proctorio.com/why-proctorio-does-not-use-facial-recognition/.
[138] *Id.*

134. Honorlock similarly represents that it does not use facial recognition.[139] Honorlock claims instead to use "facial detection" technology, "which only detects that there is a clear human face in the webcam."[140]

135. But as the FTC explained in a 2012 report, facial detection *is* facial recognition—not a separate technology. As the FTC wrote: "[C]ompanies are deploying facial recognition technologies in a wide array of contexts, reflecting a spectrum of increasing technological sophistication. *At the simplest level, the technology can be used for facial detection*; that is, merely to detect and locate a face in a photo."[141]

136. Accordingly, the "facial detection" technology that Proctorio and Honorlock use in their proctoring systems is, in fact, facial recognition.

137. Because both Proctorio and Honorlock rely on facial recognition tools to monitor students during exam sessions, both companies lack a reasonable basis to claim that they do not use facial recognition.

138. Respondents Proctorio and Honorlock have therefore engaged in unfair and deceptive trade practices in violation of D.C. Code §§ 28-3904, 28-3904(e), and 28-3904(f) and 15 U.S.C. § 45(a)(1).

139. Deceptive uses of facial recognition have previously been held to violate the FTC Act. In April 2018, EPIC and a coalition of consumer organizations filed a complaint highlighting Facebook's practice of "routinely scan[ning] photos for biometric facial matches without the consent of the image subject"—an unfair and deceptive trade practice and a violation of the Commission's 2011 consent order concerning Facebook.[142] In July 2019, the Commission determined that Facebook's use of facial recognition technology was "[d]eceptive"[143] and "misrepresent[ed] 'the extent to which a consumer can control the privacy'" of their facial data in violation of the 2011 order.[144]

D. Respondents' Claims About the Reliability of Their Test Proctoring Systems

140. Respondents represent that their online test proctoring systems can reliably detect signs of cheating.[145]

---

[139] *Student Privacy FAQ*, *supra* note 135.
[140] *Id.*
[141] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Fed. Trade Comm'n (Oct. 2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (emphasis added).
[142] EPIC Complaint, *In re Facebook, Inc. and Facial Recognition*, (Apr. 6, 2018), https://epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf.
[143] Compl. ¶¶ 144–54, *United States v. Facebook*, No. 19-2184 (D.D.C. filed July 24, 2019).
[144] *Id.* ¶ 183.
[145] *Respondus Monitor: Protecting the Integrity of Online Exams*, Respondus (2020), https://web.respondus.com/respondus-monitor-protecting-the-integrity-of-online-exams/ ("But how do you ensure the integrity of online exams and prevent cheating? The answer is with LockDown Browser

141. In fact, there is reason to believe that the systems in question are not as reliable as Respondents represent.

142. Many students subjected to these online test proctoring systems have reported groundless accusations of cheating, major technical glitches, indications of racial bias in Respondents' facial recognition algorithms, and signs that students with disabilities or atypical patterns of movement are disproportionately flagged as potential "cheaters."[146]

143. These and other reports of irregularities are a sufficient basis for the Attorney General to investigate whether Respondents can reasonably claim that their test proctoring systems reliably detect signs of cheating.

144. Respondents' unverified claims of reliability and efficacy are deceptive and thus constitute unlawful trade practices in violation of D.C. Code §§ 28-3904, 28-3904(e), and 28-3904(f) and 15 U.S.C. § 45(a)(1).

VI. Prayer for Investigation and Relief

145. EPIC urges the Office of the Attorney General for the District of Columbia to begin an investigation of test proctoring companies Respondus, ProctorU, Proctorio, Examity, and Honorlock and to find that Respondents' excessive collection of biometric and other personal data, reliance on opaque and unproven algorithms, and uses of facial recognition technology constitute unfair and deceptive trade practices under D.C. Code § 28-3904.

146. EPIC furthers urges the Office of the Attorney General to:

    a. Halt Respondents' online proctoring of students pending substantial changes in business practices;

    b. Require that Respondents make available to students the factors, logic, and determinations of AI systems used to produce assessments of test-takers;

    c. Require that Respondents make known to the students the precise basis for their evaluations;

    d. Require that Respondents comply with the requirements of the OECD AI Principles;

---

and Respondus Monitor."); *Prevention*, ProctorU (2020), https://www.proctoru.com/integrity-in-action ("Our job is to deter and prevent any breach of integrity,"); *A Comprehensive Learning Integrity Platform.*, Proctorio (2020), https://proctorio.com/ ("Using state-of-the-art technology and end-to-end data security, Proctorio ensures the total learning integrity of every assessment, every time."); *Test-taker FAQs*, Examity (2020), https://www.examity.com/test-takers/ ("[Examity] provides teachers, schools and students with the tools they need to prevent cheating and to preserve integrity."); *Provide Flexibility and Protect Your Reputation*, Honorlock (2020), https://honorlock.com/ ("At Honorlock, we have the solution you need to protect student integrity and ensure that your program's reputation remains strong.").

[146] *See* Harwell, *supra* note 79; Patil & Bromwich, *supra* note 40.

e. Require that Respondents comply with the requirements of the Universal Guidelines for AI;

f. Require Respondents to submit to annual audits of their privacy, data collection, and AI practices by an independent third party, the results of which should be publicly reported;

g. Require Respondents to create and maintain detailed logs of what types of personal data they collect, how they use such data, how long they retain such data, and whether and when they delete such data;

h. Require Respondents to provide students with access, correction, and deletion rights with respect to their own data; and

i. Provide such other relief as the Office of the Attorney General finds necessary and appropriate.

Respectfully Submitted,

/s/ Alan Butler
Alan Butler
EPIC Interim Executive Director
and General Counsel

/s/ Caitriona Fitzgerald
EPIC Interim Associate Director
and Policy Director

/s/ John Davisson
EPIC Senior Counsel

/s/ Sara Geoghegan
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)