epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Education

on

Potential New Program, from Seedlings to Scale

November 13, 2023

By notice published October 12, 2023, the Department of Education Requests information on "Potential New Program, from Seedlings to Scale."[1] The Electronic Privacy Information Center ("EPIC") writes to encourage the Department to restrict funding for any projects that use affect recognition or one-to-many facial recognition and more generally limit funding only to projects that meet rigorous privacy and security standards. As a key driver of investment in and adoption of new technologies in the education space, the Department has an obligation to ensure that those systems do not cause harm to students. EPIC is concerned that deployment of data-extractive and mistake-prone AI systems in the education space could cause significant harm, and thus demands special safeguards.

EPIC is a public interest research center established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC conducts research and advocates for common sense regulation concerning automated decision-making systems. On December 9, 2020, EPIC filed a complaint with the Office of the Attorney General for the District of Columbia alleging that five major providers of online test proctoring services have engaged in unfair and deceptive trade practices in violation of the D.C. Consumer Protection Procedures Act (DCCPPA) and the Federal Trade Commission Act. Specifically, EPIC's complaint charges that Respondus, ProctorU, Proctorio, Examity, and Honorlock have engaged in excessive collection of students' biometric and other personal data and have routinely relied on opaque, unproven, and potentially biased AI analysis to detect alleged signs of cheating.

As the Office of Educational Technology's May 2023 report "Artificial Intelligence and the Future of Teaching and Learning" recommended, the department should "Focus R&D on Addressing Context and Enhancing Trust and Safety"[1] and create "education-specific guardrails."[2]

---

[1] Department of Education Office of Education Technology, *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations* (May 2023), available at https://www2.ed.gov/documents/ai-report/ai-report.pdf at 59
[2] Id. At 60

The Department has an opportunity to put those recommendations, along with recommendations that align with the recent AI Executive Order[3], into practice. With the proper safeguards, the funds from this program can help promote student learning, bridge gaps in education quality, and preserve privacy and civil liberties.

We believe that the Department of Education should establish safeguards that guide the development and deployment of any AI technologies funded by the Seedlings to Scale program Specifically, EPIC recommends that the Department of Education:

- Only fund AI systems that use limited, curated datasets that are made public for accountability purposes. This will help reduce risks of false or inappropriate outcomes for a school setting, among other privacy violations.
- Prohibit the funding of any emotion recognition or facial recognition tools.[4]
- Require any system receiving funding to limit collection, processing, and/or transferring of the data of minors (anyone under the age of 18) to that which is strictly necessary to achieve the minor's specific purpose for interacting with the business or strictly necessary to achieve certain essential purposes that provide a clear benefit to the minor.[5]

---

[3] Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 30, 2023), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[4] *See, e.g.*, James Vincent, *Discover the Stupidity of AI Emotion Recognition with This Little Browser Game*, The Verge (Apr. 6, 2021), https://www.theverge.com/2021/4/6/22369698/ai-emotion-recognition-unscientific-emojify-web-browser-game; *see also* Kate Crawford, *Artificial Intelligence is Misreading Human Emotion*, The Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/; Charlotte Gifford, *The Problem with Emotion-Detection Technology*, The New Economy (Jun. 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology; Crawford, *supra* note **Error! Bookmark not defined.**; Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, The Conversation (Jan. 3, 2019), https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404; U.S. Gov't Accountability Off., *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial* Uses 6 (Jul. 2020), https://www.gao.gov/products/gao-20-522. [hereinafter *GAO*]; *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, Nat'l Inst. of Standards and Tech. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.; Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; Erik Learned-Miller et al., *Facial Recognition Technologies in the Wild: A Call for Federal Office*, Algorithmic Justice League 7 (May 29, 2020), https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf; Kashmir Hill, *Microsoft Plans to Eliminate Face Analysis Tools in Push for 'Responsible AI,'* N.Y. Times (Jun. 21, 2022), https://www.nytimes.com/2022/06/21/technology/microsoft-facial-recognition.html; Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. Times (Nov. 5, 2021), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html; Kate Crawford, *Time to Regulate AI That Interprets Human Emotions*, Nature (Apr. 6, 2021), https://www.nature.com/articles/d41586-021-00868-5

[5] *See e.g.* CCPA § 1798.121(a) (enumerating the purposes for which California consumers can ask a business to limit the use of their sensitive personal data to); *see also Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem,* EPIC (Nov. 2022), 167-181 https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf

- Require any developer or user of funded systems to ensure verifiable parental consent for data that is collected from minors under 13 years old, in compliance with COPPA).[6]
- Prohibit the developer or user of funded technologies from selling or otherwise transferring any data collected from minors to data brokers.
- Prohibit developer or user of funded technologies from embedding trackers into student web browsers, software, and/or devices.
- Allow parent or student to delete children's data from the technology at any time.[7]
- Require the technology to have data retention and deletion policies in place to minimize the amount of data that is collected from minors is stored.
- Require that the users of these technologies provide students and parents with an accurate list of what data it collects from students, when it collects that data, and in what manner it collects that data. This should be made in an active disclosure given to students and sent to parents, in addition to having this information embedded in the privacy policies.[8]
- Require strong cybersecurity practices, including multifactor authentication, to safeguard children's data.[9]

The use of automated systems in exam proctoring and cheating detection/suspicion applications has questionable accuracy and has caused significant harm to students. For further reading about potential negative impacts of the technologies EPIC is urging the department not to fund, EPIC recommends the following sources:

- Naiara Bellio, *200 students failed their exams. Automated proctoring could be to blame, but doubts remain*, Algorithm Watch (Jul. 18, 2023), https://algorithmwatch.org/en/spain-students-failed-blame-automated-proctoring.
- Morgan Meaker , *This student is taking on 'biased' exam software*, Wired (Apr. 5, 2023), https://www.wired.com/story/student-exam-software-bias-proctorio/
- Nora Igelnik, *Always watching: Students, instructors weigh in on Proctorio's testing surveillance and impact on mental health*, The Lantern (Jan. 9, 2023), https://www.thelantern.com/2023/01/always-watching-students-instructors-weigh-in-on-proctorios-testing-surveillance-and-impact-on-mental-health/
- Kristy P. Kennedy, *Remote Proctoring Services Are Facing Legal, Legislative Challenges*, Teen Vogue (Oct. 20, 2022) https://www.teenvogue.com/story/remote-proctoring-services-lawsuits
- Sophie Young, *Kent State changes remote testing policy in response to federal ruling*, KentWired (Sept. 12, 2022) https://kentwired.com/86613/latest-updates/kent-state-changes-remote-testing-policy-in-response-to-federal-ruling/
- Roxana Sadeghpour, *Big Proctorio is Watching You: Poorly, if You're Not White,* Woroni (Nov. 9, 2022), https://www.woroni.com.au/news/big-proctorio-is-watching-you-poorly-if-youre-not-white/

[6] Children's Online Privacy Protection Rule (COPPA) 16 C.F.R. § 312.3(b); 16 C.F.R. § 312.5
[7] 16 C.F.R. § 312.3(c); 16 C.F.R. § 312.6
[8] 16 C.F.R. § 312.3(c); 16 C.F.R. § 312.6
[9] 16 C.F.R. § 312.3(e); 16 C.F.R. § 312.8

- Aaron Gordon, *Scientists Asked Students to Try to Fool Anti-Cheating Software. They Did.,* Vice (Sept. 9, 2022) https://www.vice.com/en/article/93aqg7/scientists-asked-students-to-try-to-fool-anti-cheating-software-they-did
- Zoë Corbyn, *'I'm afraid': critics of anti-cheating technology for students hit by lawsuits,* The Guardian (Aug. 26, 2022), https://www.theguardian.com/us-news/2022/aug/26/anti-cheating-technology-students-tests-proctorio
- Amanda Holpuch and April Rubin, *Remote Scan of Students Room Before Test Violated His Privacy, Judge Rules,* New York Times (Aug. 25, 2022), https://www.nytimes.com/2022/08/25/us/remote-testing-student-home-scan-privacy.html
- Emma Bowman, *Scanning students' rooms during remote tests is unconstitutional, judge rules,* NPR (Aug. 26, 2022) https://www.npr.org/2022/08/25/1119337956/test-proctoring-room-scans-unconstitutional-cleveland-state-university
- Kashmir Hill, *Accused of Cheating by an Algorithm, and a Professor She Had Never Met*, New York Times (May 27, 2022), https://www.nytimes.com/2022/05/27/technology/college-students-cheating-software-honorlock.html
- Alec Sapolin, *Cleveland State student wins federal lawsuit against university on breach of Fourth Amendment,* Cleveland 19 (Aug. 22, 2022), https://www.cleveland19.com/2022/08/23/cleveland-state-student-wins-federal-lawsuit-against-university-breach-fourth-amendment/

As detailed above, facial recognition and emotion recognition systems have been shown to have unavoidable discriminatory impacts, as well as limited utility. For resources on the major problems caused by the widespread use of facial recognition and emotion recognition systems:

- Evan Salinger and Woodrow Hartzog, *What Happens When Employers Can Read Your Facial Expressions?,* New York Times (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html
- Minda Zetlin, *AI Is Now Analyzing Candidates Facial Expressions During Video Job Interviews*, Inc. (Feb. 28, 2018), https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html
- Woodrow Hartzog, *Facial Recognition is the Perfect Tool for Oppression*, Medium (Aug. 2, 2018), https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66
- Luke Stark, *Facial Recognition is the Plutonium of AI*, 25 XRDS 3, 50 (2019), https://static1.squarespace.com/static/59a34512c534a5fe6721d2b1/t/5cb0bf02eef1a16e422015f8/1555087116086/Facial+Recognition+is+Plutonium+-+Stark.pdf

Increased surveillance throughout the education ecosystem often interferes with learning and causes privacy and civil liberties concerns. For resources on discrimination, surveillance, and other harms of student monitoring software in general, including exam proctoring:

- *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, EPIC (Nov. 2022), 167-181, 67-108, https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf

- Drew Harwell, *Mass school closures in the wake of the coronavirus are driving a new wave of student surveillance,* The Washington Post (Apr. 1, 2020) https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/
- Mitchell Clark, *Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can't See Them*, Verge (Apr. 8, 2021) https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning
- Jason Kelley, *Canvas and other Online Learning Platforms Aren't Perfect—Just Ask Students,* Electronic Frontier Foundation Deeplinks (Apr. 27, 2022) https://www.eff.org/deeplinks/2022/04/canvas-and-other-online-learning-platforms-arent-perfect-just-ask-students
- Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students, Slate* (Feb. 24, 2022), https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html
- Jack Gillum and Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (Jun. 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/
- Rachel Kriehn, *Students Outraged at Securly Surveillance Updates,* The Arrowhead (Jan. 25, 2018), https://thearrowhead.org/5470/student-life/students-outraged-at-securly-surveillance-updates/
- Todd Feathers, *Schools Spy on Kids to Prevent Shootings, But There's No Evidence It Works*, Vice (Dec. 4, 2019) https://www.vice.com/en/article/8xwze4/schools-are-using-spyware-to-prevent-shootingsbut-theres-no-evidence-it-works
- *EFF letter to FTC on daycare apps 9-28-2022*, Electronic Frontier Foundation (Sept. 9, 2022), https://www.eff.org/document/eff-letter-ftc-daycare-apps-9-28-2022
- John Keegan and Alfred Ng, *Life360 Says It Will Stop Selling Precise Location Data*, The Markup (Jan. 27, 2022), https://themarkup.org/privacy/2022/01/27/life360-says-it-will-stop-selling-precise-location-data

EPIC remains willing and eager to discuss these priorities further as you develop your prioritizations and funding choices. Please don't hesitate to reach out to me at winters@epic.org or 202-483-1140 x 126.

Respectfully submitted,

/s/ Ben Winters
Ben Winters
EPIC Senior Counsel

/s/ Maria Villegas Bravo
Maria Villegas Bravo
EPIC Fellow