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.” 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” and create “education-specific guardrails.”

2 Id. At 60
The Department has an opportunity to put those recommendations, along with recommendations that align with the recent AI Executive Order⁵, 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

---


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).  
☐ 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.  
☐ 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.  
☐ Require strong cybersecurity practices, including multifactor authentication, to safeguard children’s data.  

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:

☐ Morgan Meaker, This student is taking on 'biased' exam software, Wired (Apr. 5, 2023), [https://www.wired.com/story/student-exam-software-bias-proctorio/](https://www.wired.com/story/student-exam-software-bias-proctorio/).  

---

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


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:


• 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-be2a08f0fe66

• Luke Stark, Facial Recognition is the Plutonium of AI, 25 XRDS 3, 50 (2019), https://static1.squarespace.com/static/59a34512c534a5fe6721d2b1/t/5cb0bf02ee1a16e422015f8/1555087116086/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:

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)

Mitchell Clark, Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can’t See Them, Verge (Apr. 8, 2021)

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


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