



December 16, 2022

STATEMENT ON PRINCIPLES FOR THE DEVELOPMENT AND DEPLOYMENT OF EQUITABLE, PRIVATE, AND SECURE REMOTE PROCTORING SYSTEMS

The ACM US Technology Policy Committee (USTPC)¹ notes that many universities, schools, and professional certification organizations have employed remote proctoring (RP) systems during the COVID-19 pandemic. Such systems are intended to permit enrolled students and other individuals taking tests (including standardized or certification examinations) to complete them by computer in their homes or other noninstitutional settings. RP systems vary in their designs and capabilities, but virtually all use software as digital exam proctors. Nearly all RP systems deploy as integrated packages that include both test-administration and -monitoring software (*i.e.*, the software both administers tests and monitors test-takers).²

Designers and providers of commercial RP systems represent that they deliver the same level of test security as achieved when tests are administered “live” in classrooms or testing centers and are proctored in person. The use of RP technology is controversial, however, among some academics

¹ The [Association for Computing Machinery](#) (ACM), with more than 100,000 members worldwide, is the world’s largest educational and scientific computing society. ACM’s [US Technology Policy Committee](#) (USTPC), currently comprising more than [175 members](#), serves as the focal point for ACM’s interaction with all branches of the U.S. government, the computing community, and the public on policy matters related to information technology. This statement’s principal author for USTPC is Christopher Kang. Primary additional contributors include Committee Chair Jeremy Epstein and Committee members Cory Doctorow, Simson Garfinkel, and Jeanna Matthews.

² The test-giving portion presents test questions, records student answers, ensures the security of the test instrument, and attempts to isolate the test computer. The test-monitoring portion attempts to ensure that the test-taker is not cheating. Some systems simply record student interactions, while others monitor the student computer’s screen or activate the student’s webcam or microphone. Many systems also augment monitoring with artificial intelligence and machine-learning algorithms designed to flag suspicious behavior for review. For example, some systems use gaze-tracking software to monitor the movement of the student’s eyes in an attempt to determine where the student is looking, which might indicate that they are using a second computer, a cell phone, or some other forbidden testing aid.

and institutions³ who question its reliability, accuracy, and racial “impartiality.”⁴ They specifically note its potential for serious adverse, sometimes egregious,⁵ effects on users’ privacy.⁶

Others have observed that because RP systems are not cost-free to acquire and deploy, educational administrators must decide whether individual test-takers must pay—and, if so, how much—to take an RP-facilitated exam.⁷ Whenever such costs are assessed to individuals, the financial inability of some to pay the fees raises critical questions that administrators must address as a matter of equity, fairness, and potentially antidiscrimination law.

³ See, e.g., Lindsey Barrett. “Rejecting Test Surveillance in Higher Education” (June 21, 2021). Available at dx.doi.org/10.2139/ssrn.3871423. The University of Illinois announced in January 2021 that it would discontinue the use of remote proctoring because of concerns raised “related to accessibility, privacy, data security and equity,” emails.illinois.edu/newsletter/1970177238.html. See also Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke, and Hannah Quay-de la Vallee. “Hidden Harms: The Misleading Promise of Monitoring Students Online,” Center for Democracy & Technology, August 3, 2022, cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/

⁴ Joy Buolamwini and Timnit Gebru. “Gender shades: Intersectional accuracy disparities in commercial gender classification,” in *Proceedings of Machine Learning Research* 81 (2018): 1–15, <https://proceedings.mlr.press/v81/buolamwini18a.html>; and [Statement on Facial Recognition Technologies](#), ACM US Technology Policy Committee (June 30, 2020). See also Katherine L. Gibson and Jonathan M. Smith, “The emperor’s new masks: On demographic differences and disguises,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (2015): 57–64, https://openaccess.thecvf.com/content_cvpr_workshops_2015/W02/html/Gibson_The_Emperors_New_2015_CVPR_paper.html

⁵ Pia Ceres. “Kids Are Back in Classrooms and Laptops Are Still Spying on Them,” *Wired*, August 3, 2022, www.wired.com/story/student-monitoring-software-privacy-in-schools/

⁶ Universities and other organizations employing RP must comply with a range of federal statutes, including the Family Educational Rights and Privacy Act (FERPA), Individuals with Disabilities Education Act (IDEA), guidance provided directly by the Department of Education, and Section 508 of the Rehabilitation Act of 1973 when the software is used by a U.S. government entity. This creates a complex legal and regulatory environment that administrators must navigate. Administrators must decide not just which RP platforms to use but also which features to enable and how to respond to the concerns of students and faculty. See Andy Dua. “Using Human Intervention and Technology to Secure Test-Taking,” *Forbes*, May 4, 2021, www.forbes.com/sites/forbesbusinesscouncil/2021/05/04/using-human-intervention-and-technology-to-secure-test-taking

Furthermore, recent rulings call the legality of broad-based data collection into question. See, e.g., *Ogletree v. Cleveland State University*, No. 1:21-CV-00500, United States District Court Northern District of Ohio Eastern Division, August 22, 2022, <https://www.courthousenews.com/wp-content/uploads/2022/08/500.pdf>. See also Ashley Belanger. “Scanning Students’ Homes During Remote Testing Is Unconstitutional, Judge Says,” *Ars Technica*, August 23, 2022, <https://arstechnica.com/tech-policy/2022/08/privacy-win-for-students-home-scans-during-remote-exams-deemed-unconstitutional>

⁷ The pricing structure for RP systems is often also opaque. Costs range from an estimated \$4 per hour per test to \$15 per hour per test, and more for platforms that require more complex monitoring. See, e.g., Jean Dimeo. “[Online Exam Proctoring Catches Cheaters, Raises Concerns](#),” *Inside Higher Ed*, May 10, 2017, www.insidehighered.com/digital-learning/article/2017/05/10/online-exam-proctoring-catches-cheaters-raises-concerns

Such issues also arise whenever RP systems and associated institutional policies for their use⁸ require test-takers to have access to a computer, Wi-Fi, and/or broadband internet service, and/or to be alone in a room for the duration of an exam. It frequently is not possible, for example, for homeless and otherwise economically disadvantaged students and test-takers to satisfy these requirements. These issues notwithstanding, the use of RP technology is forecast to expand⁹ because of both the increased flexibility and perceived cost savings it offers educational and other test-administering institutions.¹⁰

In the committee's view, as RP technologies emerge as a pervasive component of online education, institutions and technology vendors at a minimum¹¹ must address major issues of equity, privacy, security, accessibility, and efficacy.¹² To that end, USTPC offers these guiding principles:¹³

EQUITY

- Remote proctoring systems must be fair to all test-takers. A common feature of RP tools is that they provide some form of virtual inspection of the student's environment during test-taking. This can produce inequitable outcomes to the disproportionate detriment of already marginalized learners, including:
 - *Homeless test-takers.* These students may have no choice but to take tests in cafés or parking lots within range of libraries or other public Wi-Fi hot spots. RP technologies typically deem these environments unacceptable, often without the possibility of appeal.

⁸ USTPC believes that policies regarding the use of RP should be effective, understandable to test-takers, and privacy-conscious in keeping with ACM's [Code of Ethics and Professional Conduct](#), which counsels computing professionals to avoid harm, be cognizant of the public good, and thoroughly evaluate the impacts and risks of computing systems before deploying them. While written for ACM members and other computing professionals, these core precepts of the code also may be employed by policy makers assessing how to effectively regulate development and use of RP technologies.

⁹ See, e.g., Nora Caplan-Bricker. "[Is Online Test-Monitoring Here to Stay?](#)," *New Yorker*, May 27, 2021, www.newyorker.com/tech/annals-of-technology/is-online-test-monitoring-here-to-stay

¹⁰ Institutions also may be motivated to permanently adopt online or hybrid online/in-person learning strategies to expand their enrollments and their appeal to previously underrepresented and nontraditional students.

¹¹ The issues addressed by these principles are not comprehensive. Others, including nontechnical considerations, should also concern policymakers. These include, for example, resolving whether parents must consent to the vendor-dictated terms of service for their minor child's use of RP software, and what standards of disclosure and layperson comprehensibility will influence or dictate the content of such terms of service.

¹² While beyond the scope of this statement, the committee also notes that the application of RP technologies may simultaneously embolden the implementation of other surveillance systems (e.g., employee monitoring software). See Jodi Kantor and Arya Sundaram. "The Rise of the Worker Productivity Score," *New York Times*, August 14, 2022, www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html

¹³ The committee's analysis and recommendations pertain to automated monitoring systems while recognizing that they may also well be relevant to systems that at least partially rely on human monitoring. The latter are likely to be designed and deployed much less frequently because they are costly and difficult to operate successfully at scale.

- *Test-takers in broadband deserts.* Some housed students have inadequate or no access to sufficiently robust broadband internet service to meet baseline RP requirements or to fully enable such systems. They, too, must take their exams in environments that RP tools reject. Previous work has found that access to broadband is strongly correlated with a person's race and economic status.¹⁴
- *Test-takers in crowded homes.* Many test-takers live in quarters where every room is necessarily occupied by at least one other person, often a person who cannot reasonably be expected to move, such as a parent working the night shift whose sleep cannot be interrupted during a remote exam. Not only can such students face immediate disqualification for failing to isolate themselves, but the very act of requiring them to show their environment to instructors or remote proctors is an invasion of both their privacy and the privacy of others with whom they share living space.
- Any deployed RP system, and the policies that govern its use, must accommodate these and similar cases without prejudice to the test-taker.
- RP technologies may have system requirements that exceed those of some students' equipment, which often is configured only as minimally needed for students to play video games or participate in online discussion.¹⁵ Such requirements for hardware and high-performance internet connectivity may preclude some students from utilizing these systems.¹⁶ RP vendors and institutions thus must ensure that system requirements are comparable to prior course requirements without imposing onerous technical burdens on students. Institutions considering the use of RP technologies should also ensure that, when operating in resource-constrained environments (such as on older laptops or computers with less-than-optimal memory), users' experience of the software's operation will not be distracting to them or functionally degraded in material ways.¹⁷
- Institutions should ensure that all students, regardless of their ability to pay associated fees, have full access to institutionally mandated RP systems.¹⁸

¹⁴ Lara Fishbane and Adie Tomer. "Neighborhood Broadband Data Makes It Clear: We Need an Agenda to Fight Digital Poverty," *Brookings*, February 6, 2020, www.brookings.edu/blog/the-avenue/2020/02/05/neighborhood-broadband-data-makes-it-clear-we-need-an-agenda-to-fight-digital-poverty/

¹⁵ For example, many systems simultaneously transmit two video streams—the video camera and the desktop—as well as run image-processing software on the test-taker's system.

¹⁶ More broadly, testing systems may be incompatible or unstable on certain devices for a variety of reasons. For example, they may not be designed to work with newer processors. Emma Roth. "Intel's 12th Gen CPU Can't Handle the Bar Exam," *The Verge*, July 13, 2022, www.theverge.com/2022/7/13/23209784/intel-law-students-12th-gen-processor-bar-exam-exemplify-examsoft

¹⁷ Prior to enrolling in a class, the requirements needed to use RP systems should be made clear and students should be provided with a means of verifying without cost that they can successfully use any required RP system.

¹⁸ The committee notes that such accommodations are routinely made by institutions, such as when laboratory fees are waived based on financial hardship and sees no rationale for treating required software differently.

PRIVACY

- Data collection by RP technologies should be targeted, transparent, and minimized. Collected data should be retained for at most one year following the conclusion of the student's tenure at the educational institution.¹⁹
- Test-takers using RP technologies must, at minimum,²⁰ be provided notices describing:
 - What data will be collected and how long it will be retained
 - Who will have access to data (*e.g.*, administrators, automated systems, or teaching assistants)
 - How information collected may be used in determining academic misconduct
- Test responses should be segregated from non-test response data. Non-test response data includes audio and visual recordings of the test-taker, and technical information (*e.g.*, the test-taker's IP address and keystroke timing data). Access to these kinds of data should be independently controlled and logged.
- Data collected by RP technologies, especially sensitive data such as video and audio recordings, should be destroyed when they are no longer required by administrators. RP vendors should never retain data for any purpose, even if the material is anonymized or students are given the ability to "opt out" of such data retention.
- RP technologies should incorporate end-to-end encryption for all test-taking data,²¹ both in transit and at rest.
- RP technologies should not access the local data on the test-taker's computer. For example, the technologies should not scan the test-taker's files in an attempt to locate unauthorized copies of testing materials.²² Likewise, RP technologies should not include remote control features, such as the ability to move the test-taker's mouse, select other windows, or enter keystrokes on the test-taker's computer.²³

¹⁹ A substantially shorter period may well be more appropriate, particularly when improper test-taker activity is not reasonably suspected or is determined not to have occurred.

²⁰ Whenever technically feasible, as it ought to be in most cases, the committee also strongly recommends that RP system designers engineer systems to provide test-takers with visual previews of how the RP software will perceive their environments that flag items the software could or would consider violative of the exam's protocols so that they may be redressed before the start of the remotely proctored test. Such features must be made fully compatible with audio description programs relied upon by visually impaired students.

²¹ Test-taking data includes responses, data collected as a result of monitoring, and test-taking metadata (such as IP addresses, mouse movements, and keystroke intervals).

²² See Note 5.

²³ Although vendors may find it tempting to build remote control "help desk" functions into their products, the potential for abuse is too great; many other safer modalities are available for test-takers who require such support.

- RP technologies must be designed to automatically disable all tracking functions once exams for which they are employed have been completed. Such software also should provide test-takers with a transparent mechanism to easily and totally disable installed RP software as well as to wholly remove it from the test-taker's computer.
- Data collected by RP technologies, including but not limited to screenshots and video/audio recordings, should be considered educational records under the Family Educational Rights and Privacy Act (FERPA),²⁴ and institutions should be prepared to promptly share all information collected by RP technologies with students, as required by law, upon a student's request.
- While FERPA provides a process for resolving student privacy violations, this process applies only to students and parents. Therefore, educational institutions and RP vendors should also adopt policies to protect whistleblowers who report privacy violations or security vulnerabilities in RP platforms.
- When enforcement actions are taken against test-takers suspected of academic misconduct, institutions must voluntarily share all information pertinent to that determination with the accused, including but not limited to the relevant data collected by RP technologies. Users of RP technologies should be especially mindful of relying upon the conclusions of AI systems to support claims of misconduct if the underlying AI technology has not been subject to rigorous peer review.²⁵
- Policies should be amended or adopted to address directly how collected data will be used to resolve allegations of academic misconduct, and how the institution will maintain compliance with FERPA and all other applicable laws and regulations.²⁶ These policies should be freely accessible for students to review prior to course enrollment. Ideally, they should also be standardized within an institution or department.

SECURITY

- Security must be a primary design objective of all RP software. Accordingly, prior breaches of RP systems²⁷ and reports that RP vendors have threatened or filed suit against individuals who have complained about their products²⁸ are particularly troubling.

²⁴ www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

²⁵ Indeed, the committee notes that outside the U.S., sole reliance on automated decision-making could well be illegal. See, e.g., Article 22.1 of the European Union's General Data Privacy Regulation.

²⁶ Institutions, for example, may have to modify their document retention policies to accommodate online class recordings, chats, and discussion boards to comply with applicable federal and disparate state laws.

²⁷ See, e.g., Thomas Germain. "Poor Security at Online Proctoring Company May Have Put Student Data at Risk," Consumer Reports, December 10, 2020, www.consumerreports.org/digital-security/poor-security-at-online-proctoring-company-proctortrack-may-have-put-student-data-at-risk

²⁸ See, e.g., "EFF Sues Proctorio on Behalf of Student It Falsely Accused of Copyright Infringement to Get Critical Tweets Taken Down," press release, April 21, 2021, www.eff.org/press/releases/eff-sues-proctorio-behalf-student-it-falsely-accused-copyright-infringement-get

- Institutions procuring RP software should require affirmative statements that vendors will not suppress warnings about defects in their products, will promptly disclose known product vulnerabilities, and will issue software updates as frequently as needed to minimize cyber risk.
- Vendors should adopt an affirmative public disclosure and bug bounty program, and commit to not use copyright, cybersecurity, or confidentiality claims to silence legitimate criticism, particularly from educators and students.
- As noted above with respect to privacy, RP technologies should incorporate end-to-end encryption for all test-taking data,²⁹ both in transit and at rest.

ACCESSIBILITY

- RP vendors must ensure that their systems are accessible to all potential users, including users with disabilities and those who have limited equipment or internet connectivity.
- Test-takers who require special accommodations must be able to fully and equitably utilize RP technology. Institutions' RP systems must allow the use of assistive technology and not inappropriately identify students making use of authorized accommodations.
- RP technologies should be designed to respect behaviors that may be suspicious in neurotypical test-takers, but may be involuntary in others (*e.g.*, looking around the room). For institutions, this could require human adjudication of flagged behaviors. For vendors, this dictates that neurodiverse training sets should be used for automated systems.

EFFICACY

- Educators, researchers, and technology providers should develop uniform benchmarks and certification procedures to assess and document the comparative effectiveness of RP systems in identifying students receiving unauthorized help, whether with the aid of physical notes, other websites, or other people present at the testing location.
- Given that RP technologies depend on automated systems whose accuracy has often been proven to be substantially reduced by bias, particularly with respect to race and gender,³⁰ such systems and the institutional policies governing their use must provide means to appeal determinations by automated systems to a human for re-adjudication.
- Vendors thus should train and test their software on a wide range of complexions, hairstyles, body types, etc., and publish the results of these tests for educational institutions, students,

²⁹ Test-taking data includes responses, data collected as a result of monitoring, and test-taking metadata (such as IP addresses, mouse movements, and keystroke intervals).

³⁰ See Note 4.

and independent researchers³¹ to review. Similarly, RP vendors should be required to test their software with both neurotypical and neurodiverse students. The committee also urges that questionnaires and all other user-facing materials intrinsic to RP software be gender neutral in their composition.

USTPC also recommends that practices, policies, rules, and statutes governing the development and deployment of all RP technology be consistent with its Statements on [Statement on Algorithmic Transparency and Accountability](#),³² [Joint Statement on Principles for Responsible Algorithmic Systems](#),³³ and [Statement on the Importance of Preserving Personal Privacy](#).³⁴

³¹ Given the broad impact that RP technologies are likely to have on academia and industry certification processes, and the millions of people engaged in them, the research community should monitor the adoption of RP technologies and, as the data may dictate, periodically make science-based recommendations for their refinement and use.

³² www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

³³ <https://www.acm.org/binaries/content/assets/public-policy/final-joint-ai-statement-update.pdf>

³⁴ www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf