August 12, 2021

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

The ACM U.S. Technology Policy Committee (USTPC)[1] notes that many universities, schools, and professional certification organizations employed remote test administration (RTA) 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 non-institutional settings. RTA systems vary in their designs and capabilities, but virtually all use software as digital exam proctors.[2]

Designers and providers of commercial RTA systems represent that they deliver the same level of test security and repeatability as achieved when tests are administered "live" in classrooms or testing centers and are proctored in person. The use of RTA technology is controversial, however, among some academics and institutions[3] who question its reliability,

---

[1] The Association for Computing Machinery (ACM), with more than 100,000 members worldwide, is the world's largest educational and scientific computing society. It is dedicated to uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM's US Technology Policy Committee (USTPC), currently comprising more than 130 members, serves as the focal point for ACM's interaction with all branches of the US 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] Nearly all RTA systems deploy as integrated packages that include both test-administration and monitoring software. That is, the software performs both test-giving and tester-monitoring. The test-giving portion present test questions, record student answers, ensure the security of the test instrument, and attempts to isolate the test computer. The tester-monitoring portion attempts to ensure that the test-tasker 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. Furthermore, many systems augment the 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 eyeballs in an attempt to determine where the student is looking, which might indicate that the student is using a second computer, a cell phone, or some other forbidden testing aid.

[3] See, e.g., Barrett, Lindsey, Rejecting Test Surveillance in Higher Education (June 21, 2021). Available at SSRN: ssrn.com/abstract=3871423 or dx.doi.org/10.2139/ssrn.3871423. Note that the University of Illinois announced in January 2021 that it would discontinue the use of remote proctoring because of concerns that had been raised "related to accessibility, privacy, data security and equity." [emails.illinois.edu/newsletter/1970177238.html.]

ACM U.S. Technology Policy Committee
1701 Pennsylvania Ave NW, Suite 200
Washington, DC 20006

+1 202.580.6555
acmpo@acm.org
www.acm.org/public-policy/ustpc

accuracy, racial "impartiality,"[4] and note particularly its potentially adverse effects on users' privacy.[5]

Others also have observed that, because RTA systems are not free to acquire and deploy, educational administrators must decide whether or to what degree individual test-takers must pay to take an RTA-facilitated examination[6]. Whenever such costs are assessed to individuals, the financial inability of some to pay such fees raises critical questions that administrators must address as a matter of equity, fairness, and potentially anti-discrimination law.

Such issues also will arise whenever RTA systems and associated institutional policies for their use[7] 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 examination. It frequently will not be possible for homeless and otherwise economically disadvantaged students and test-takers to satisfy these requirements.

These issues notwithstanding, the use of RTA technology is forecast to expand[8] because of both the increased flexibility and perceived cost savings it offers educational and other test-administering institutions.[9]

---

[4] See Note 21, below.

[5] Universities and other organizations employing RTA 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 RTA platforms to use, but which features to enable, and how to respond to the concerns of students and faculty. See, 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]

[6] The pricing structure for RTA systems is often also opaque. Costs range from an estimated $4 per hour per test to $15 per hour per test, or more for platforms that require more complex monitoring. See, e.g., 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]

[7] USTPC believes that policies regarding the use of RTA 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 the development and use of RTA technologies. [www.acm.org/code-of-ethics]

[8] See, e.g., 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]

[9] Institutions also may be motivated to permanently adopt online or hybrid online/in-person learning strategies in order to expand their enrollments and their appeal to previously underrepresented and non-traditional students.

As RTA technologies emerge as a pervasive component of online education, **in the Committee's view institutions and technology vendors at minimum must address major issues of equity, privacy, security, accessibility, and efficacy**.[10]

To that end, USTPC offers the following guiding principles:

EQUITY

- A common feature of RTA tools is that they provide some form of virtual inspection of the student's environment during test-taking. We have observed that this produces inequitable outcomes to the disproportionate detriment of already-marginalized learners:
    - *Homeless test-takers***.** These students may take tests in cafes, parking lots within range of libraries or other public Wi-Fi hotspots. RTA technologies typically deem these environments to be unacceptable, often without the possibility of appeal;
    - *Test-takers in broadband deserts***.** Some housed students have no or inadequate access to sufficiently robust broadband internet service to meet baseline RTA requirements or fully enable such systems. They, too, must sit their exams in environments that RTA tools reject out of hand. Previous work has found that access to broadband is strongly correlated with a person's race and economic status;[11] and
    - *Test-takers in crowded homes***.** Many test-takers live in quarters where every room necessarily is occupied by at least one other person in it, often a person with nowhere else to go or who cannot reasonably be expected to move, such as a nightshift working parent whose sleep cannot be interrupted during an 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 invasive both to their privacy and the privacy of others with whom they share living space.
- Any deployed RTA system, and the policies that govern its use, must accommodate these and similar cases without prejudice to the test-taker.

---

[10] This list is not exclusive. Other issues, including non-technical considerations, also should 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 RTA software, and what standards of disclosure and layperson comprehensibility will influence or mandate the content of such Terms of Service.

[11] "Neighborhood broadband data make it clear: We need an agenda to fight digital poverty," Lara Fishbane and Adie Tomer, 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/]

- RTA technologies may have system requirements that exceed those of some students, which often are limited to those needed for students to play video games or participate in online discussion.[12] Such requirements for hardware and high-performance internet connectivity may preclude some students from utilizing these systems. RTA vendors and institutions must assure system requirements are comparable to prior course requirements. Institutions considering the use of RTA technologies also should assure 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 or materially functionally degraded.[13]

- Institutions also should ensure that all students, regardless of their ability to pay associated fees, will have full access to institutionally mandated RTA systems.[14]

PRIVACY

- Data collection by RTA technologies should be targeted, minimized, and transparent. Collected data should be retained for at most one year following the conclusion of the student's tenure at the educational institution.

- Test-takers using RTA technologies must be provided notices describing:
  - What data will be collected and how long the data will be retained;
  - Who will have access to data (e.g. administrators, automated systems, or teaching assistants); and
  - How information collected may be used in making a determination of 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 each of these kinds of data should be independently controlled and logged.

- Data collected by RTA technologies, especially sensitive data such as video and audio recordings, should be destroyed when they are no longer required by administrators. RTA vendors should never retain data for any purpose, such as product improvement, even if the material is anonymized or if students are given the ability to "opt-out" of such data retention.

---

[12] 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.

[13] Prior to enrolling in a class, the requirements needed to use RTA systems should be made clear. There should be some mechanism for students to verify without cost that they can successfully use any required RTA system.

[14] 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 than, for example, reagents, test tubes and flasks.

- RTA technologies should incorporate end-to-end encryption for all test-taking data,[15] both in transit and at rest.

- RTA 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. Likewise, RTA 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-tasker's computer.[16]

- RTA technologies must provide test-takers with a mechanism to quickly, easily and totally remove the RTA software from the test-taker's computers and wholly disable any ongoing tracking functionality.

- Data collected by RTA technologies, including (but not limited to) screenshots and video/audio recordings, should be considered educational records under FERPA,[17] and institutions should be prepared to promptly share all information collected by RTA technologies with students, as required by law, upon a student's request.

- While FERPA provides a process for resolving student privacy violations, this process only applies to students and parents. Educational institutions and RTA vendors should therefore adopt policies to protect whistleblowers who report privacy violations or security vulnerabilities in RTA platforms.

- When enforcement actions are taken against test-takers suspected of academic misconduct, institutions must voluntarily share all pertinent information for that determination with the accused, including (but not limited to) the relevant data collected by RTA technologies. Users of RTA technologies should be especially mindful of using conclusions of AI systems to support claims of misconduct if the underlying AI technology has not been subject to rigorous peer review.

- Policies should be amended or adopted to directly address 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.[18] These policies should be freely accessible for students to review prior to course enrollment. Ideally, they also should be standardized within an institution or department.

---

[15] "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).

[16] 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 modalities are available for test-takers that require help desk support.

[17] www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[18] 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.

SECURITY

- Security must be a primary design objective of all RTA software. Accordingly, prior breaches of RTA systems,[19] and reports that RTA vendors have threatened or filed suit against individuals who have complained about their products,[20] are particularly troubling.
- Institutions procuring RTA software should require affirmative statements that vendors will not suppress warnings about defects in their products.
- Vendors should adopt an affirmative public disclosure and bug bounty program, and they should promise not to use copyright, cybersecurity or confidentiality claims to silence legitimate criticism, particularly from educators and students.
- As noted above with respect to Privacy, RTA technologies should incorporate end-to-end encryption for all test-taking data,[21] both in transit and at rest.

ACCESSIBILITY

- RTA vendors must assure that their systems are accessible to all potential users, including users with disabilities, and those who have limited equipment or weak Internet connectivity.
- Test-takers who require special accommodations must be able to fully and equitably utilize RTA technology. Institutions must verify that their chosen RTA systems allow the use of assistive technology and do not inappropriately identify students making use of authorized accommodations.
- RTA 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 adjudications of flagged behaviors. For vendors, this dictates that neurodiverse training sets should be used for automated systems.

---

[19] See, e.g., 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]

[20] See, e.g., EFF Sues Proctorio on Behalf of Student It Falsely Accused of Copyright Infringement to Get Critical Tweets Taken Down, *Electronic Frontier Foundation* (April 21, 2021). [www.eff.org/press/releases/eff-sues-proctorio-behalf-student-it-falsely-accused-copyright-infringement-get]

[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).

EFFICACY

- Educators, researchers, and technology providers should develop uniform benchmarks and certification procedures to assess and document the comparative effectiveness of RTA systems in identifying students receiving unauthorized help, whether with the aid of physical notes, access to other websites, or other people present at the testing location.

- Given that RTA technologies depend on automated systems the accuracy of which often have been proven to be substantially reduced by bias, particularly with respect to race and gender,[22] such systems and the institutional policies governing their deployment must provide mechanisms to appeal determinations by automated systems to a human for re-adjudication. RTA vendors also should be required to train and test their software on a wide diversity of complexion ranges, hair styles, body types, etc. and to publish the results of these tests for educational institutions, students and independent researchers[23] to review. Similarly, RTA vendors should be required to test their software with both neurotypical and non-neurotypical students. The Committee also urges that questionnaires and all other user-facing materials intrinsic to RTA software be gender neutral in their composition.

USTPC also recommends that practices, policies, rules and statutes governing the development and deployment of all RTA technology be consistent with its Statement on Algorithmic Transparency and Accountability and Statement on the Importance of Preserving Personal Privacy.[24]

[22] Facial recognition software is routinely less effective in accurately identifying women and people of color. *See:* Joy Buolamwini, Timnit Gebru. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*. 2018; and Statement on Facial Recognition Technologies, ACM US Technology Policy Committee (June 30, 2020). [www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf]

[23] Given the broad impact that RTA 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 RTA technologies and, as the data may dictate, periodically make science-based recommendations for their refinement and usage.

[24] Both Statements are available online at, respectively: www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf, and www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf.