Privacy Considerations for Remote Proctoring Technology
DRAFT May 13, 2020

Requiring students to turn on their camera and be recorded in their private home during an exam poses privacy concerns and should be undertaken with care and transparency. Both national and local media have reported on how these concerns have accelerated during the COVID pandemic.

We recommend instructors exhaust feasible alternatives, before opting for remote proctoring technologies. *If* remote proctoring is chosen, please consider adopting the recommendations in this guidance.

Thank you to numerous faculty including Professor Cynthia Carter Ching (Education), Professor Elizabeth Joh (Law), Professor Matt Bishop (Computer Science), and Professor Phillip Rogaway (Computer Science) for their review and input on drafts of this guidance.

Note: Guidance can be updated to reflect additional input. Please email privacy@ucdavis.edu if you have suggestions or requests. This guidance does not address cybersecurity questions such as whether the remote proctoring software is secure. Contact cybersecurity@ucdavis.edu for those questions. This guidance also does not provide a "how-to" guide on using the technology. Contact your College's IT Unit for those questions.

1. ***Since any proctoring is a form of surveillance, how are remote proctoring privacy concerns different from live proctoring privacy concerns?***

Unlike live proctoring in a public classroom, remote proctoring monitors a student in their private home or bedroom. Some technologies even require that students pan the camera around the bedroom, exposing their entire private space. The student is recorded in close-up for an extended period of time. And, videos of the student can be stored for long periods, well beyond the exam period, increasing the risk of unauthorized access.

Remote proctoring technologies like Examity and Respondus Monitor rely on, store, process[1], or record biometric images of the student (such as facial characteristics, retina and iris patterns, voiceprints) for AI-enabled automated recognition. While collected for legitimate educational purposes (such as detecting whether the recorded student is the same student throughout the session), students have expressed concerns over the potential for misuse.

Some students have also expressed discomfort or anxiety with close-up recordings being kept by an instructor or video monitored by a stranger (Examity employs live proctors located in another country). Students living in small homes or with multiple family members may have less or no access to a private setting.

2. ***What are the equity and inaccuracy concerns with remote proctoring technologies?***

[1] Respondus Monitor's Privacy Policy states that they use facial detection and facial recognition technology to automatically process recorded facial images during the exam session. The Policy further states that a "biometric signature" of the user is "generated and used temporarily, but the signature is not stored on Respondus servers." No definition of biometric signature was provided.

Remote proctoring technologies like Examity and Respondus Monitor rely in part on artificial intelligence to flag body movements and the momentary presence of others as potential cheating indicators. Poor Internet connectivity or an interruption by a pet or sibling in a crowded household could be misinterpreted by software as cheating. The New York Times has reported on how other routine body movements could be falsely flagged as cheating.

If a student has poor internet connectivity, low bandwidth, or limited computer hardware (no webcam; a computer without video capacity), instructors should not require Examity. If a student does not have a computer with video capability or a webcam, an instructor should explore with the student whether campus tech aid resources can resolve the problem.

3. What privacy safeguards should I adopt before using remote proctoring technology?

- **Explore all Feasible Alternatives Before Opting for Digital Proctoring**

Consider using the Privacy Balancing Process (see FAQ 8 below) and related resources to assess whether student privacy risks outweigh the benefits of testing integrity. The process suggests first exhausting feasible alternatives, as a part of that balancing process.

- **Provide Clear and Transparent Notice to Students Well Before the Exam**

  - Instructors should advise students well in advance of technology ground rules (e.g. no interruptions; no excessive movements or stretch breaks; recorded sessions; terms of use) and requirements (stable, high bandwidth; video capability; no chromebooks).

  - Advise students of personal data collected and advise that the session will be recorded. This notice must be well in advance of exam day. A sample notice could be:

    "This program records you during the exam session. Recorded session data includes your facial characteristics and related biometric records, voiceprint, any picture ID, and your immediate surroundings during the exam to facilitate the test environment. Recorded data may be used at UC Davis solely for the purpose of verifying test environment integrity. Any vendor is prohibited from redisclosing this information, except as required by law or permitted by the Vendor's Privacy Policy."

  - Advise students of applicable data deletion rules. Zoom relies on the instructor to decide when data is deleted. Examity's default storage period is 60 days, unless the video is flagged. Examity states that students may also request that Examity delete data once that information is no longer needed by UC Davis. Requests can be emailed to info@examity.com or received via phone at 855-392-6489.

  - Remind students of campus mental health resources that are available to them if they find themselves experiencing more than normal anxiety over the exam process.

  - Be clear that if certain activities (neglect, domestic violence) are witnessed in the background, any UCD employee who witnesses the activity must or may (depending on the activity) report those activities to campus authorities.

- **Offer An Option to Request an Alternative**

- Ensure students have ample time to request accommodations for relevant disabilities.

- Permit students to petition for an alternative arrangement. Sample alternative arrangements include:

    - Opportunity to petition for an alternative exam method, such as a take-home exam, a paper, or other alternative, and identify an example list of circumstances that might qualify for such an alternative (e.g. reasonable accommodation, low bandwidth situation, lack of a private room, high risk of interruption; high risk of excess body movement (sneezing from allergies)).
    - For Zoom proctoring where students can view each other, allow a student to use an advance-approved alternative to their full name, such as the student's initials, the student's first name or last name only.
    - For proctoring that relies on AI-enabled automated flags, survey your students to assess constraints (low bandwidth; sneezing allergies) that could be falsely flagged as cheating by the technology; log these constraints with the technology vendor, in advance of the exam.

- **Develop Clear Post-Exam Criteria and Advice**

Instructors can be clear on what recourse students have if there is a no-fault error during the timed exam (accidental disruption by a pet or a child; internet disruption, etc.). Students with a legitimate disruption should have the opportunity to explain what happened and receive a rescheduled test or an alternative exam.

4. ***If Zoom is used for remote proctoring, instructors must adopt measures to avoid "outing" students with disabilities to other students in the class.***

Instructors must take precautions to ensure their use of Zoom for remote proctoring does not permit other students to identify students who have been given accommodations for disabilities (e.g., students who need extra time). This would be a privacy violation because it discloses personal information about a student's disabilities. To avoid this problem when using Zoom, you may need to use a Zoom breakout room or run concurrent, multiple Zoom sessions. The campus Student Disability Specialist offers Zoom support to faculty members on responding to accommodations requests or you can send an email to examaccom@ucdavis.edu.

5. ***Have Respondus Monitor, Examity and Zoom been evaluated by the University for privacy concerns?***

Zoom. Campus guidance on Zoom privacy and its Privacy Policy can be found at FAQ 16 here

Examity. Personal information Examity collects include a student's name, a video copy of a student's identification card, geolocation data, and biometric student information. Biometric student information is defined by Examity as "one or more biological or behavioral characteristics that can be used for automated recognition, such as facial characteristics, retina and iris patterns, voiceprints." Some media have scrutinized Examity's proctoring platform and privacy risks related to the biometric information.

Examity states that student data is not sold or rented but may be disclosed to a third party for a Business Purpose (defined as "to assist in providing the service, to process payments, or to provide customer assistance") or in certain other circumstances such as legal requirements, lawful requests by public authorities, corporate mergers.

Contact the Campus Information Security Office at cybersecurity@ucdavis.edu for information on whether Examity's security protections are adequate to protect higher sensitivity stored data.

Respondus Monitor. Unlike Examity which can rely on a mix of live proctors and AI-enabled software, Respondus does not hire any personnel to live proctor. Instead, Respondus relies solely on AI-enabled algorithms to flag images. Instructors may in their discretion later view recordings that have been flagged.

The campus privacy and security assessment of Respondus is being reviewed and the campus contract with Respondus is under development. Currently, Respondus online Privacy Policy states that "random samples of video and/or audio recordings may be collected by Respondus … and shared with researchers under contract with Respondus." The statement suggests that such research would be limited to improving Respondus' services.

Other than research purposes, Respondus states that it does not share student video information with third parties (other than the Institution, the student, parents), except Respondus will share information to comply with law, to respond to a governmental authority, or to remove information that violates its terms.

6. Is exam video data stored? For how long? Who may access this stored video?

On campus, only the instructors, individuals authorized by the instructor (such as a TA), and campus officials with a FERPA-compliant purpose (such as to adjudicate academic misconduct allegations) may view the recordings. Both Examity and Zoom reserve the right to view recordings to comply with requests from legal authorities or to service the product.

Examity. Examity's default policy is to store video recordings for 60 days, except for flagged cases which are stored for one year. The Privacy Office has requested a copy of the Examity contract to assess whether the campus applied a different data storage period. This guidance will be updated once that contract is received.

Zoom. The instructor and individuals authorized by the instructor control when Zoom recordings are deleted. To minimize the risk and liability of unauthorized disclosures of stored videos, instructors should delete recordings once they are no longer needed for their original testing purpose.

Some UCD colleges have set "automatic deletion" settings for all recordings after a certain number of days. Some units have established 100 days as the automatic deletion period. Recordings should be deleted once they are no longer needed for their educational purpose.

Respondus Monitor. Respondus' default policy is to store video recordings for 5 years. The campus can request that this period be curtailed to a shorter period. The Privacy Office has requested a copy of the Respondus contract to assess whether a different storage period was contractually applied. This guidance will be updated once that contract is received.

7. ***Instructors should not independently purchase proctoring products using click-through agreements, rather than using campus-approved products.***

Campus-approved products have been assessed to ensure compliance with federal and state laws and UC policies related to procurement, FERPA, security, accessibility, protection of faculty intellectual property, protection of medical privacy, and protection of California residents' privacy. Given the high sensitivity level of video data in remote proctoring, using a non campus-approved product for remote proctoring is not allowed.

8. ***In deciding whether to adopt remote proctoring technology for my exam, how do I assess whether the benefits of remote proctoring prevail over the burdens and privacy risks?***

The UC Privacy Balancing Process is one method that can be used to assess whether benefits outweigh privacy intrusion risks.

A balancing decision depends on the specifics of each case. A few factors to consider in that balancing:

- What are the limits of the technology (e.g. high bandwidth only; webcam; video)? Are most of your students' exam conditions able to overcome those limits? See "Using Remotely Proctored Assessments" here for a list of limits for Examity and Zoom.
- Are alternative exam approaches feasible? See "Alternative Assesesments" here and an example of one faculty member's recommendations here for instructor alternatives to digital proctoring of exams, as well as here for support on student accommodations requests.
- What reasonable privacy protections have you made available? See the guidance noted earlier in this document.
- What are the privacy risks of the remote proctoring technology? See guidance noted in this document.

9. ***If a UC Davis instructor inadvertently views prohibited activities (domestic violence, criminal activity), what are the reporting obligations?***

All University employees are required to report sexual harassment or sexual violence they are aware of that involves a student to the University's Title IX Office. Such reports can be made to the Harassment & Discrimination Assistance and Prevention Program (HDAPP) by emailing hdapp@ucdavis.edu, or to the Title IX Officer by emailing wjdelmendo@ucdavis.edu.

Faculty are also required to report academic misconduct to the University by contacting the Office of Student Conduct and Judicial Affairs at ossja@ucdavis.edu. While employees are not required to report other forms of student misconduct to OSSJA, they may do so by contacting the same email address.

Some University employees are mandatory reporters for purposes of reporting child abuse and neglect. In addition to reporting child abuse and neglect to the appropriate authorities, reports should also be made to the University when the abuse or neglect arises in connection with a University program. Employees who are not mandated reporters are encouraged to report suspected child abuse or neglect when it is related to a University

program. Such reports can be made by contacting wjdelmendo@ucdavis.edu or filing a report on the University's whistleblower hotline.