Insights, News & Events

TEST INTEGRITY IN THE REMOTE LEARNING ERA: HOW YOUR SCHOOL CAN AVOID PRIVACY VIOLATIONS

Insights
Sep 7, 2022

A federal judge in Ohio just concluded that a university's practice of conducting room scans for remote testing was unreasonable and a violation of a student's Fourth Amendment privacy rights. The August 22 decision in *Ogletree v. Cleveland State University* is sure to serve as a word of warning for schools across the country anxious to avoid a similar fate. After all, we've seen an increased emphasis on security measures for tests and quizzes over the past several years. From K-12 to graduate school programs, there are a variety of options to protect the integrity of graded assessments, and the choices for doing so grow year after year. Test performance data is used in a variety of ways, and every school should be concerned with protecting the validity of that data. Your school may have procedures for distributing, collecting, and returning test materials, might require exam software that blocks all other programs, or could utilize a plagiarism detection system – but has your school thought about whether your test security measures affect your students' privacy rights?

Factual Background

Cleveland State University, even before COVID-19, offered some remote courses and developed a procedure manual to protect the integrity of remote tests. The school had some required test security practices for every course. It also had a number of recommended security practices which were up to the discretion of each faculty member, including the use of remote proctoring tools designed to safeguard test security. Although recorded room scans were not a specific

Related People

Jenna B. Rubin
Partner
404.260.3410

Service Focus

Litigation and Trials

Privacy and Cyber

Industry Focus

Education

recommended practice, two of the school's recommended remote proctoring programs required a room scan in the opening instructions.

When using the remote proctoring programs for an online exam, Cleveland State University students would first show their ID to the camera next to their face so that a live proctor or proctoring application could verify that the person taking the test was the same person that appeared in the ID. Next, the proctoring program or live proctor would prompt students to conduct a room scan of the testing environment.

Students taking the remote test could see the room scans of other students. The student in this case, Aaron Ogletree, was notified two hours before a test that there would be a room scan. He replied that he had confidential documents in his test area and did not have time to secure them. At the start of the test, he was asked to conduct the room scan, and he complied. The scan lasted less than one minute.

Ogletree filed suit against the school and alleged that the school's practice for remote test takers to use their camera to briefly scan the test area violated his rights under the Fourth Amendment as an unreasonable search.

Court's Analysis

Because remote room scans have not been previously examined under the Fourth Amendment, the court analyzed each element of a Fourth Amendment violation:

1. Is a remote virtual room scan a search under the Fourth Amendment?
   The first element of a search under the Fourth Amendment is whether there is a subjective expectation of privacy that society deems "reasonable." Notwithstanding the school's argument that the use of room scans was standard practice with remote proctoring programs, the court answered this question with a resounding "yes." This expectation of privacy in the home is the heart of the Fourth Amendment.

   Yet, the court pulled back a bit and explained that if a virtual room scan was not a search under the Fourth Amendment, it would be difficult to determine what legal standard would govern a room scan. This concerned the

court, as there could be far-reaching implications for other areas that "interact" with technology.

2. Is a remote virtual room scan reasonable under the Fourth Amendment?
   The court next considered whether the room scans were reasonable. Although suspicion-less searches are generally prohibited under the Fourth Amendment, there is an exception if the government — or in this case public university — has "special needs" which must be balanced against the individual's privacy expectations.

   There are four factors to balance when considering whether a special needs exception applies: 1) the nature of the privacy interest; 2) the character of the intrusion; 3) the nature and immediacy of the government's concern; and 4) the efficacy of the intrusion as a means of addressing that concern.

The Court's Conclusion

The court balanced the student's privacy interest in his home (and, in particular, his bedroom where the test was taken), the inconsistency of the school's test security procedures, the discretion given to faculty members to implement remote testing, the school's move to online only courses in the face of the COVID-19 pandemic, the minimally intrusive nature of the room scan, the school's interest in preserving the integrity of its tests, the other safeguards available to protect test security, and the ways in which room scans did not protect test security.

Even though the court hemmed and hawed a bit about its conclusion, it found that there were other procedural safeguards that would serve the same purpose as the room scan. It also found there were ways to still cheat even with a room scan, such as cheating when leaving the room for a bathroom break. It also found that the school's "sporadic and discretionary use of room scans" demonstrated that the room scans were not truly effective at preserving test integrity. Accordingly, the court concluded that the room scans were unreasonable searches under the Fourth Amendment.

Lessons Learned

Even though this case involved a Fourth Amendment analysis of room scans because the issue involved a public

university, almost every state has modeled its common law invasion of privacy claims on the Fourth Amendment. So, although this case was limited to the "government" (charter schools, public schools, public universities, etc.), the same analysis could be used in a claim against a private entity as well under a common law invasion of privacy theory.

The easiest way to avoid this type of claim is to not use room scans as a requirement for remote testing. There are many other remote testing security measures available. There are software programs that can record how long a student spent on an exam, log what IP address they used to log in, block the student from using the internet or accessing other programs during the test, or flag suspicious activity. Schools should be cautious about any measure that involves recording a student in their home – an area that the courts have long held are uniquely private.

One of the weakest parts of the school's argument in this case was the inconsistency in use of remote testing security measures. When developing your school's remote testing security measures, be thoughtful about the reason for a particular security measure and work to ensure that it is applied to all courses and students. Even one exception will cast doubt on the usefulness, efficacy, and necessity of the security measure.

Conclusion

We will monitor these developments and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox. If you have further questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our Education Practice Group.