Student Surveillance and the Student Test-Taker Privacy Protection Act

In the last two years, online proctoring companies have seen a 500% increase in their usage. A survey by EDUCAUSE in 2020 indicated that more than half of higher education institutions use remote proctoring services and another 23% are considering doing so.

This data collection goes far beyond what is required for the functionality of the service. Students rarely have an ability to opt out. One study showed that 97% of students using online proctoring tools were required to do so. Indeed, students often don't know that proctoring companies have collected their data and retain it for years. No current state privacy law adequately protects students from these practices. **We urge the legislature to require proctoring companies to practice data minimization, and limit them to collecting only what is necessary to offer their services.**

We must protect students who have no choice but to use online proctoring tools from predatory and dangerous data collection. Large collections of PI create the risk of a security breach and resulting fraud. Moreover, once a proctoring company has collected this personal data, companies frequently monetize it by disclosing it to a wide variety of other entities, including "group companies," third-party marketing partners, and other third-party service providers and partners. Additionally, proctoring companies can disclose this data to law enforcement, national security, immigration enforcement, and other government entities. All of this exposure opens test takers to a variety of privacy and security risks. For more information about the dangers of overcollection of data, read EFF's blog post, "Stop Invasive Remote Proctoring: Pass California's Student Test Taker Privacy Protection Act."

Proctoring companies' egregious data processing practices have already resulted in harm to students:

- ProctorU is being sued for violating the Illinois Biometric Information Privacy Act (BIPA), after a data breach affected nearly 500,000 users. The lawsuit states biometric data from the breach dated back over eight years.
- The Electronic Privacy Information Center (EPIC) filed a complaint with the D.C. Attorney General's office against five online proctoring services due to the unjustified, excessive, and harmful data collection used on students who have no meaningful opportunity to opt out.
- In 2020, the California Supreme Court directed the California state bar to prepare a timetable for destruction of all examinees' PI retained by the proctoring company contracted to remotely proctor the California State Bar exam (ExamSoft). The court recognized that some data collection was unrelated to the administration of the bar, and that unnecessary retention of sensitive PI increases the risk of unintentional disclosure.

Data minimization is the solution. State law must prohibit proctoring companies from processing more PI than is strictly needed to provide a proctoring service. And it must empower test takers to enforce their privacy rights against proctoring services that break the law.

Suggestions for Legislative Language:

> 1. When a business provides proctoring services in any educational setting, it shall only collect, retain, disclose, and use information as strictly necessary to provide that proctoring service.
>
> 2. If a business violates this section, then any consumer subjected to that violation may institute a civil action against that business. A prevailing party may recover: (a) liquidated damages of $1,000 per consumer per incident or actual damages, whichever is greater; (b) injunctive and declaratory relief; and (c) reasonable attorney fees and costs, including expert witness fees.

Want more information? Please contact Hayley Tsukayama at **hayleyt@eff.org** or Chao Jun Liu at **chao@eff.org**