

# Hidden Harms: Student Activity Monitoring After *Roe v. Wade*

## What is student activity monitoring?

[Student activity monitoring software](#) is any technology that tracks students' activity online, such as dates and times of logins to systems, the contents of students' screens, or the contents of their emails, chats, or search and browsing history. Student activity monitoring may also enable real-time visibility into what students are looking at on their computers and can occur within a learning management system or through a separate software program. Monitoring has resulted in widespread collection and sharing of students' online activity; in [research](#) by CDT, 44 percent of teachers report that a student in their schools was [contacted by law enforcement](#) because of student activity monitoring, 37 percent of teachers reported that their school sends alerts to law enforcement outside of school hours, and [29 percent of LGBTQ+ students](#) report that they or someone they know has been outed by this technology.

## How did *Dobbs* affect students' privacy rights when being monitored?

In June 2022, the Supreme Court issued its decision in [Dobbs v. Jackson Women's Health Organization](#), overturning the federally protected right to obtain an abortion once guaranteed by [Roe v. Wade](#). *Roe*, however, was not just about abortion, but also privacy, and its conception of privacy and autonomy protected students and minors, including [confidentiality](#) in reproductive healthcare decisions and regarding their [sexual orientation and gender identity](#).

With the legal matter returned to states, policymakers have begun enacting and enforcing laws regarding reproductive health, including [criminalizing abortions](#). Because student activity monitoring is often trained to look for sexually explicit material, it is possible that reproductive health information is already being [collected and shared with law enforcement](#), which could be used to prosecute students seeking access to [reproductive care](#), as well as people they communicate with who assist them. Schools, state law enforcement, and other authorities may even ask vendors to [add keywords](#) related to reproductive health. Monitoring software provides schools unprecedented glimpses into students' lives, including regarding reproductive healthcare decisions; the overturning of *Roe* now provides law enforcement with reason to access that data.

## What about FERPA and HIPAA?

Two federal laws — the [Family Educational Rights and Privacy Act \(FERPA\)](#) and the [Health Insurance Portability and Accountability Act \(HIPAA\)](#) — do not protect students' reproductive healthcare information from student activity monitoring:

- **FERPA** does little to address the student data that schools collect, and generally provides schools broad flexibility in sharing that information with “[school officials](#),” including technology contractors or even school resource officers or law enforcement. Moreover, FERPA permits disclosures to law enforcement in [compliance with a court order or subpoena](#) or for [health and safety emergencies](#), making it possible for states that have criminalized reproductive healthcare to obtain student data from schools.
- **HIPAA** likely provides few protections for students; [HIPAA does not apply to “education records”](#) covered by FERPA, and [few schools are subject to HIPAA](#). Data collected from student activity monitoring, such as browsing history, might reveal students' reproductive healthcare choices, but are not medical records protected by HIPAA. Even if monitoring data were covered by HIPAA, it permits, but does not require, covered entities to respond [to law enforcement demands](#).
- [State laws](#) may offer protections for students' privacy and reproductive healthcare decisions — or criminalize those decisions and threaten their privacy.

## What can schools do to protect students?


Schools can [take measures to protect their students](#):


- **Minimize data sharing and collection:** Schools should not proactively or automatically share student data regarding reproductive healthcare with law enforcement. If a district chooses to use monitoring software, it should minimize the data collected by ensuring that data related to reproductive healthcare is not collected or retained and by limiting monitoring to certain times or activities.
- **Transparency:** If districts choose to use student activity monitoring, they should inform parents *and students* about the specific data collected and how it is used and shared.
- **Maintain control of student data:** Schools and districts should make explicit in their contracts with vendors that they, rather than the vendors, have ultimate control of student data. Schools should instruct vendors to neither collect nor retain data related to reproductive healthcare and in any event to not proactively disclose such data to law enforcement or other third parties. Retaining control over student data is required by FERPA and reduces the risk of exposing students to harmful data uses.
- **Build capacity within the school community to protect students:** As an alternative to student activity monitoring, districts can engage community members to monitor students' online activities and coach them on digital literacy and online citizenship, which can limit the unnecessary collection of data about students.

**For more information  
from this research, see  
CDT's recent report on  
the promises and perils  
of student activity  
monitoring software,  
*Hidden Harms.***

 [cdt.org](https://cdt.org)

 [cdt.org/contact](mailto:cdt.org/contact)

 Center for Democracy & Technology  
1401 K Street NW, Suite 200  
Washington, D.C. 20005

 202-637-9800

 @CenDemTech

