DATA PRIVACY & GOVERNANCE HUB

Utah Law Strengthens Student Privacy Protections for Educational Technology

SEPTEMBER 3, 2026

Key Takeaways

- Researchers at Brigham Young University (BYU) reported that some educational technology (EdTech) applications used in Utah K-12 schools collected and shared student data in ways that violated privacy agreements.
- Utah House Bill 55, which took effect on July 1, 2026, increased privacy requirements for EdTech vendors by allowing educational institutions to conduct audits and terminate contracts if privacy violations persist for 30 days after being addressed.
- The results raise issues about how well schools and EdTech vendors can safeguard children's digital privacy.

What Happened

As educational technology grows in K-12, numerous apps are now used for learning in educational facilities. However, while these technologies benefit learning, they raise privacy concerns about how student information is collected and shared. Following an investigation commissioned by the Utah State Board of Education, BYU professors Mark Keith and Justin Giboney, together with a team of student researchers and the nonprofit Internet Safety Labs, analyzed network traffic from 100 educational apps most commonly used in Utah schools. To do so, the researchers created test student accounts and analyzed about 15-20 minutes of activity in each app. The study found that 52% of EdTech companies that had signed data privacy agreements collected student information not permitted by those agreements, 36% shared it with advertisers, and some even used unique identifiers for digital profiling.

Privacy and Governance Concerns

The major privacy concern is the collection and disclosure of children's personal information through education applications. While schools may have agreements and privacy requirements governing how vendors handle information, the BYU study found that some companies collected data even when they had such agreements. The researchers found that 36% of EdTech companies with data privacy agreements shared data with advertisers and even used unique identifiers for digital profiling.

Additionally, the problem illustrates the gap between privacy requirements and vendors' actions in collecting children's data. Federal protections include the Children's Online Privacy Protection Act (COPPA). The Utah Student Data Protection Act also provides privacy requirements for children's data. However, based on the BYU findings, privacy requirements and written agreements may not be enough without ways to verify compliance.

Why It Matters / Policy Considerations

The policy issue shows the need to move beyond privacy agreements in contracts toward verification. Schools and other educational organizations might not have the capacity to independently verify whether all the applications they adopt meet the privacy policies that they set. Based on this, BYU researchers suggested that schools adopt a "trust but verify" strategy: review network traffic first, then audit after adopting an application.

H.B. 55 in Utah provides for auditing and contract termination when violations are not addressed within 30 days. However, the problem also raises issues of consistency across states. Because education technology is used nationwide, students may receive different levels of privacy protection depending on which state they attend school in. More transparency about what information EdTech firms collect, who receives it, and how long they store it would improve accountability. Periodic compliance audits, data minimization guidelines, vendor reporting, and penalties for violations would also help. The BYU scholars hope Utah's approach will inspire other states to do the same.