Pennsylvania Senate Communications and Technology Committee
and Senate Educational Committee
Joint Public Hearing on Student Data Privacy
Tuesday, October 18, 2022
10:30 a.m.

Testimony by Linnette Attai, President and Founder
PlayWell, LLC Privacy Consulting

Chairwomen Phillips-Hill and Williams, Chairmen Martin and Kane, and Members of the Committees, it is an honor to be here today to speak with you about protecting student data privacy.

I'm Linnette Attai, President and Founder of PlayWell, LLC. I am a data privacy consultant with more than 20 years of experience advising companies and non-profit organizations around the globe on managing their data privacy responsibilities in relation to United States, European Union, and United Kingdom requirements. I do similar work for US K-12 educational institutions. In the simplest terms, I help organizations build their data privacy programs in support of lawful and ethical use of personal information.

My work involves a special focus on and expertise in youth and student data privacy. I am the author of one of the Children's Online Privacy Protection Act (COPPA) safe harbor programs approved by the Federal Trade Commission, and of three books designed to educate US K-12 educational institution technology leaders and teachers about protecting student data privacy.

In addition, I serve as the Student Data Privacy Program Director for the Consortium of School Networking (CoSN), the national organization supporting K-12 educational technology leaders. In that capacity, I spearhead the creation of free student data privacy resources and manage the Trusted Learning Environment privacy framework for K-12 educational institutions and state educational agencies.

Protecting the privacy and security of student data is a critical requirement for educational institutions and for the third-party service providers, including technology companies, that support them. We all can appreciate that the information security risk profile across educational institutions is high relative to that of other sectors,[1] and that K-12 educational institutions are particularly appealing targets for cyberattackers.[2] While there are complex

[1] https://www.databreachtoday.com/blogs/what-industry-most-vulnerable-to-cyberattack-p-3283
[2] https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions and

factors that drive this situation, under-resourced privacy programs and security programs contribute to and exacerbate the issues.

Thus, it is important to understand that the path forward to mitigate risk and protect student personal information is often a very painstaking and a very human endeavor. It requires that educational institutions engage in the challenging work of creating organizational functions adequately resourced to build, implement, maintain and grow mature data privacy and security programs.

For educational institutions, I consider this work part of their "duty of care" to students.

For third party service providers, including for-profit and non-profit technology providers and the array of nonprofit community service organizations that work in partnership with educational institutions, building mature data privacy and security programs is part of a set of fundamental requirements for operating in the sector and for the privilege of collecting and processing student personal information.

The expectations for educational institutions on this front are high, as are the challenges. To properly protect student data privacy and mitigate risk, educational institutions must work to establish and maintain organization-wide policies and procedures that govern the collection, use, maintenance, sharing, and protection of student personal information and implement associated controls in a manner that is consistent with legal requirements and community expectations. To accomplish this with any success requires establishing cross-departmental understanding of the requirements across existing laws and driving organizational change to support consistent and meaningful implementation of and adherence to privacy norms.

The typical K-12 educational institution is often alone in amassing the resources, knowledge, and expertise for such an endeavor. Many K-12 educational institutions do not enjoy the benefit of employing individuals experienced in and dedicated to both data privacy and data security.[3] Those that do often are led by a technology professional who may be self-taught in these rather complex disciplines. While the US Department of Education's Privacy Technical Assistance Center (PTAC),[4] the US Cybersecurity & Infrastructure Security Agency (CISA),[5] and nonprofit member organizations work to help fill that gap, the chasm is wide.

Legislative efforts can and do support improvements in student data privacy protections. However, they should be considered with regard for existing educational institution practices

https://www.cisa.gov/uscert/ncas/alerts/aa22-249a

[3] https://www.edsurge.com/news/2019-02-25-chief-privacy-officers-the-unicorns-of-k-12-educational

[4] https://studentprivacy.ed.gov/

[5] https://www.cisa.gov/schools

and third-party service provider operations that work in partnership with the educational institutions under the limitations set forth in FERPA. Then still, the aim should be to guide improvements in student data privacy protections while avoiding or mitigating unintended, adverse consequences that may make it more difficult for educational institutions to fulfill their fundamental purposes and requirements. Here, it can be helpful to draw from existing data privacy fundamentals,[6] including those incorporated in current legislation.

The current landscape of student data privacy legislation is complex. At the federal level, it includes, but is not limited to, the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment, privacy provisions in the Individuals with Disabilities in Education Act and the National Student Lunch Act, and, where applicable for technology providers, COPPA. Higher educational institutions and certification entities typically operate in the context of additional data privacy laws that apply to their student communities, including consumer health and financial data protection laws. (Note that most US state student data privacy laws address protections for student personal information in K-12 educational institutions.)

Across the United States, there are currently upwards of 130 K-12 state student data privacy laws. Throughout the course of drafting and implementing that legislation, there have been a variety of lessons learned, a few of which are referenced here. For example:

- Attempts to require educational institutions to obtain consent from parents and eligible students prior to sharing any student personal information could effectively shut down an educational institution's ability to operate, including its ability to record student attendance, grades, and basic identity details in a student information system. This type of consent requirement can also prevent students from taking advantage of a variety of opportunities, including participating in a yearbook, engaging in certain curricular activities, and being considered for scholarship awards.[7]
- Requiring educational institutions to publish contracts with third-party service providers without redaction may provide a roadmap for threat actors looking for student personal information.
- Depending on the nature of the information being provided, giving parents and students additional forms does not always equate to meaningful transparency.[8]

[6] https://www.fpc.gov/resources/fipps/
[7] https://www.fedscoop.com/are-student-privacy-laws-hurting-students/
[8] https://dataqualitycampaign.org/resources/flagship-resources/show-me-the-data-2022/

A more constructive path forward is to focus on educational institution data governance requirements that drive improvements across internal organizational privacy practices, combined with sensible limitations on use of student personal information for purposes that support educational institution interests. This approach supports stronger privacy protections while also reinforcing boundaries for responsible partnerships with third-party service providers. It also often reinforces existing federal requirements to provide parents and eligible students with rights to access and request correction of errors in a student's educational record.

This approach furthers the reasonable and responsible collection and use of student personal information while not limiting the ability of educational institutions and states to implement effective educational practices, improve educational outcomes, and support workforce readiness. This is particularly important today, when in the wake of global pandemic shifts, meaningful education data is necessary to develop solutions to educational challenges that many are only just beginning to understand.[9]

The "school officials" provision of FERPA[10] is a particularly important support for this work. It serves as a useful guide when working to ensure that educational institutions are able to operate responsibly and effectively with third-party service providers for both administrative and educational purposes while maintaining control over the use and maintenance of student personal information and the integrity of the educational record within an ecosystem that is also transparent with parents and students.

Student data privacy legislation must also be drafted to recognize that when educational institutions share student personal information with third parties, those institutions are typically establishing a direct business relationship with the third parties as service providers. Each third-party service provider is then governed by and beholden to its relationship with the institution. The institution drives its requirements in relation to protection and use of student personal information and is often best-positioned to manage the relationships with parents and students with regards to the educational record.

Understanding these relational constructs also helps in avoiding unintended operational disruptions for both educational institutions and third-party service providers that support the institutions with a range of services, including those necessary to provide curricular materials, deliver on personalized learning programs, act as a platform of record, provide food services or transportation, analyze organizational and educational effectiveness, and more.

[9] See https://www.gao.gov/products/gao-22-105816 and https://ies.ed.gov/schoolsurvey/spp/
[10] 20 U.S.C. § 1232g; 34 CFR Part 99, Section 99.31(a)(1)(B)

As an added note, when considering bans on collection of specific data elements, assessing current educational institution use cases for those elements can be a helpful exercise to inform decisions.[11] With that information in hand, decisions can be made about whether existing concerns may be able to be tempered with meaningful use limitations and protection requirements, including access and retention limitations. Similarly, understanding industry-standard frameworks for information breach response and reporting can inform and support timely and appropriate notification to impacted parties and oversight agencies while not interfering with the need to prioritize the critical containment and remediation processes.

With respect to enforcement provisions, it is difficult to find examples of existing enforcement actions, but drafting models to support the legislative intentions behind enforcement do exist. In short, it's necessary to establish a clear enforcement mechanism from an agency with the authority to enforce over impacted entities, the knowledge and expertise necessary to understand the existing and distinct legal requirements for various types of educational institutions and third-party service providers with respect to both federal and state laws, and the resources to properly address violations. Some states rely on their existing business and professions codes for enforcement against technology providers and other covered business entities, with enforcement against educational institutions being more effectively served by educational agencies.

One of the most important considerations for student data privacy legislation is appreciating the challenges of implementation for educational institutions. Existing US state student data privacy laws impose significant obligations on K-12 educational institutions, including development and implementation of data privacy and data security programs, establishment of data stewards, imposition of additional administrative and reporting responsibilities, and enhanced transparency requirements. These are often imposed without accompanying guidance or funding. For educational institutions, particularly those in the K-12 system, identifying resources in the form of time, training, and expertise to understand and implement requirements can be burdensome.[12]

The need to protect student data privacy is equaled only by the need to provide educational institutions with sensible, actionable guidance and resources to accomplish the work. This emphasis on resources for educational institutions is critical for ensuring legal compliance, growth and maintenance of data privacy and security programs over time, and maturity of

[11] See https://www.govtech.com/data/state-legislatures-grappling-with-biometrics-use-in-schools.html and https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8318548/

[12] https://portal.ct.gov/-/media/DAS/CTEdTech/publications/2021/CET2021K-12StaffDevices.pdf

practices across educational institutions in building effective and responsible partnerships with their third-party service providers.

When considering legislative efforts, I encourage attention to the following:

1. Ensure that requirements do not conflict with or lessen the strength of existing federal requirements, particularly the school officials provision of FERPA and the educational institution's control over the educational record.

2. Consider requirements that would meaningfully improve student data privacy protections by supporting improved privacy governance and establishing broader frameworks for appropriate data use, while avoiding unintended consequences, including interference with fundamental operations and imposition of administrative burdens that do not further privacy objectives.

3. Consider the potential impacts of legislation with regard to the diversity of both the educational institution and third-party service provider ecosystems.

4. Ensure an effective, authorized, knowledgeable, and resourced enforcement authority.

5. Provide effective resources to support educational institution compliance

I applaud the work of both Committees in providing this forum to discuss the needs and further explore pathways to support the privacy of student personal information. I am happy to remain available to Committee members in furtherance of this work.