Testimony of the
Pennsylvania School Boards Association

Before the
Senate Education Committee
and
Senate Communications and Technology Committee

Regarding
Student Data Privacy and Protection

October 18, 2022

Presented by
Charlie Reisinger, M.S.
Chief Information Officer
Penn Manor School District

Chairwoman Phillips-Hill, Chairman Kane, Chairman Martin, Chairwoman Willams, and members of the Committees; thank you for the opportunity to share the experiences and challenges faced by school districts through our Commonwealth to address student data privacy, protection, and security. My name is Charlie Reisinger. I currently serve as the Chief Information Officer of the Penn Manor School District in Lancaster County. We serve 5500 students in 10 buildings across 110 square miles. Penn Manor is a diverse district in terms of socioeconomic status, racial/ethical composition, and student learning needs.

This is my 25th year serving in public education in Pennsylvania. Most of my career has been in educational technology leadership. As a proud product of Pennsylvania public education, I am a living example

of someone with one of those *future jobs* that never existed when I was a high school student. I've been fortunate to be a part of the technology revolution that dramatically improved teaching and learning, and created incredible career opportunities for students. Without question, the technology revolution is one of the most substantial, and beneficial, changes to public education in the last 100 years.

October is Cybersecurity Awareness Month, so our student data privacy and protection discussion is especially timely. To help frame the digital data discussion, consider that technology is threaded deeply into every part of public education. **A student's 12 year academic career generates a huge digital footprint that begins in kindergarten and follows through to commencement, and beyond.** You've probably heard the term *Big Data*. Pennsylvania's schools have it sitting in server rooms, classrooms, and online educational systems.

The data includes personal details and contacts, assessments, assignments, grades, homework, health records, attendance history, discipline records, special education records, communications, PSSA, PVAAS, PIMS records, and more. It's a staggering amount of private data for schools to manage, maintain, and protect. And the volume of data grows every day.

Here's *one* example to illustrate the enormity of the data archive. Every school year, Pennsylvania public school districts are required to report 42 data sets to the Pennsylvania Department of Education's PIMS system[1]. These data sets contain dozens of data points per student. For our district's 5500 Penn Manor students, this process amounts to millions of private data records stored in both our local student information systems and the PDE PIMS data warehouse.

Our rich treasure chest of student data is of particular financial interest to cyber criminals. It can be used as leverage to extort school districts as part of a ransomware heist. Or a criminal can threaten to release confidential and highly personal student information on the open web.

Adult identity theft is a serious issue—and it's even worse for students who might not discover the problem for a decade or more. The first time a student may discover her identity has been stolen could be when she applies for college financial aid, or a car loan. Imagine being 18 and hearing that your credit was already ruined by a criminal who stole your personal information while you were in 4th grade.

---

[1] https://www.education.pa.gov/DataAndReporting/PIMS/ManualsCalendar/Pages/default.aspx

At the start of the 2022-23 academic year, the Los Angeles Unified School District suffered a massive ransomware cyberattack that exposed more than 400,000 private student records, including health and psychological evaluation records. A criminal gang, known as Vice Society, claimed the attack. Vice Society also claimed responsibility for a similar attack in September at Moon Area School District in Allegheny County.[2]

Incidentally, the timing is no surprise—the opening of schools is also open season for cyber criminals. School staff are at their absolute busiest time in August and September. Schools are much easier targets when staff and teachers are working overtime to welcome students back from summer break.

In response to these attacks, schools across the country recently received a joint cybersecurity advisory by The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA)[3] warning of an accelerating number of ransomware and cyber attacks on K12 schools.

Penn Manor is not immune to attacks. On the Friday before our first student day, I was pulled away from leading a teacher workshop to learn of an attack on our district network infrastructure. A still unidentified criminal attempted to break into our network firewall. After many hours of work and mitigation, my team successfully stopped the attack. However, dealing with the incident pulled staff resources away from helping teachers just as they prepared for the first day of school.

Penn Manor staff work hard to protect student data and prevent catastrophic cyber events. Our core tech team is small and lean—only 7 individuals provide technical support for 10 schools, 5500 students, 700 teachers and staff, 7000 devices, and hundreds of software applications. We have no full-time dedicated cybersecurity personnel. However, we are constantly fighting a 10,000 pound, multi-headed, data security monster. Unlike our staff, the monster never sleeps. It kicks at our network doors and rattles our digital locks 24 hours a day, 7 days a week. There are no days off or holidays.

- Penn Manor's website has been subjected to more than 206,000 brute force login attempts.
- Hourly, our district firewall regularly prevents more than 65,000 nefarious connections from non-U.S. computer networks.

[2] https://www.bleepingcomputer.com/news/security/vice-society-claims-lausd-ransomware-attack-theft-of-500gb-of-data/
[3] https://www.cisa.gov/uscert/ncas/alerts/aa22-249a

- District staff and students received more than 2700 suspicious email messages during September 2022. Of those, more than 500 were targeted phishing attempts.

These attacks originate from all corners of the globe. Typically, they are motivated by profit. Some are small-time thieves. Others are organized cybercriminal operations with sophisticated infrastructure, advanced technical arsenals, and even customer service departments ready to help facilitate ransomware payments. Many operate overseas, well out of the reach from state or U.S. law enforcement jurisdictions.

Scams and cyber attacks are relentless, sophisticated, and challenging to mitigate. In response, the need for skilled technology and cybersecurity talent has exploded. However, our inability to keep pace with compensation typical in business and industry leaves us with few qualified applicants. This is not an unfamiliar experience—schools have long struggled with finding and keeping qualified technology talent. What *is* new is the frequency and complexity of the cyber attacks, especially ransomware.

Cybersecurity is the most pressing concern, but it's not the only issue affecting student data privacy and protection. Students and teachers regularly use hundreds of educational websites and online services as part of their instruction. These websites add another dimension to the privacy and protection equation.
Each website must be vetted and monitored for both instructional fidelity and how the site deals with personal student information. Key questions include:

- Can learners archive, save, or import and export content or activity data in a variety of formats?
- Are the site's encryption policies and practices clearly communicated and updated?
- Does the website clearly state what personal data is collected?
- How is the student instructional data used and shared?
- How do parents consent to information collection?
- What student analytics and behaviors are collected?
- Do students maintain ownership and copyright of their intellectual property/data?
- Can the student keep her data private and decide if/how data is to be shared?
- How are data breaches handled? Who is notified and when?

Although Pennsylvania does not have student data privacy regulations, the federal Children's Online Protection and Privacy Act (COPPA) provides some safeguards. COPPA imposes requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or

online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.[4]

COPPA was a firm step in the right direction. However, it leaves a gap in protection for students between the ages of 13 and 17. In addition, the ruling was enacted in 1998, 25 years ago. 1998: Remember the 500 pound monitors and the chipper "You've got mail!" greetings? COPPA regulations are still tied to the era of AOL and Windows 98, and technology has moved on.

One example of post-1998 technology developments is **dark patterns**—website interfaces that subtly influence our behavior. Dark patterns are used to manipulate us into giving up personal information, or to desensitize us to shady privacy practices. You've probably encountered some of the following examples:

- Emotional language crafted to encourage oversharing of personal information
- A nagging prompt constantly requesting a phone number or email
- Convoluted navigation that makes it difficult to find the site privacy policy
- Confusing privacy controls, or color choices that make it difficult to spot privacy settings
- Language tricks: "Uncheck this box if you don't want to great personal recommendations"

Dark patterns are just one of many techniques used to influence and manipulate our online behavior. And students are often ill-equipped to spot them. School internet safety curriculum typically focuses on online stranger danger. Few school districts provide robust lessons in cyber self-defense or understanding data privacy.

While the challenges to school cybersecurity and data privacy are serious, there are actions we can take to better protect all Pennsylvania students and families. I have four recommendations:

One: Opportunities exist for creative partnerships between commonwealth organizations. Millersville University of Pennsylvania is next to Penn Manor High School. Our two institutions have a long history of working together on educational and technology efforts to benefit our community. Millersville University is renowned for teacher education, and they are expanding a new undergraduate program in information technology and cybersecurity. **I encourage the members of this committee to explore options that would accelerate cyber partnerships between public schools and the State System of Higher Education.** This

[4] https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

could take the form of internships, job knowledge exchange, apprenticeships, and other practical, skills-focused initiatives to support schools, as well as business and industry.

Two: The state currently provides school entities with guidance, resources and best practices with regards to **physical school safety and security**. Yet somewhere along the way, we failed to include a **digital safety**, privacy, and protection strategy for all students, teachers, and parents. **I encourage the committee to consider creating a commonwealth Student Data Privacy Office which could provide schools with guidance and resources related to digital safety, privacy, and protection**.

Three: Pennsylvania can act with intention to protect the online privacy of students under the age of 18. The recent California Age-Appropriate Design Code Act (AADC)[5] is a model for how a law may work for Pennsylvania. AADC requires online businesses that provide products or services to those under 18 years old to prioritize the safety of children. **I encourage the committee to explore similar legislation to create a child-safe internet for students in Pennsylvania.**

Four: Pennsylvania has a unique funding opportunity at this moment. The Department of Homeland Security (DHS) announced the **State and Local Cybersecurity Grant Program** (SLCGP), a first of its kind grant program to address cybersecurity risks and threats to information systems owned or operated by—or on behalf of—state and local. Through the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress established the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program, appropriating $1 billion to be awarded over four years.[6] **I encourage members of this committee to seize the opportunity for funding new programs and protections for students and school districts.**

Thank you for your interest in this topic. Pennsylvania students and parents deserve assurance that their private digital footprint remains private, and their schools remain digitally secure. This is a complex and an urgent issue in our school systems. But I believe we can work collaboratively to boost school cybersecurity into an orbit similar to physical security. I am happy to take your questions and comments.

Charlie Reisinger, M.S.

[5] https://www.wired.com/story/california-aadc-kids-privacy-age-checks/
[6] https://www.cisa.gov/cybergrants

Chief Information Officer
Penn Manor School District
Lancaster County, Pennsylvania
www.pennmanor.net

Noted PA Cyber incidents 2021-22

- **March 2021:** Altoona Area School District - Criminals captured 150GBs of data including social security numbers and health information.[7]
- **October 2021**: Corry Area School District - A ransomware attack exposed confidential student and staff personal information, including social security numbers.[8]
- **September 2022**: Mars Area School District suffered a breach just a few weeks ago.[9]
- **September 2022**: Moon Area School District[10]

[7] https://www.wtaj.com/news/local-news/altoona-school-district-releases-details-in-cyber-attack/
[8] https://www.govtech.com/education/k-12/corry-schools-need-months-to-deal-with-ransomware-attack
[9] https://www.butlereagle.com/20221004/mars-area-still-addressing-cybersecurity-issue/
[10] https://www.wtae.com/article/moon-area-school-district-hit-by-cyberattack/40968745