Protecting Privacy in Connected Learning

March 15, 2017

Sheryl Abshire, Ph.D.
@sherylabshire

sheryl.abshire@cpsb.org
Chief Technology Officer – CoSN Board
Calcasieu Parish Public Schools
Lake Charles, Louisiana

Transforming Education Through Visionary Technology Leadership

- About CoSN:
  - Premier professional association for K-12 school system education and technology leaders
  - Providing management, community building, and advocacy tools you need to succeed
  - Representing over 13 million students in school districts nationwide
  - Empowering educational leaders to create and grow engaging learning environments

Student Data Privacy

- Why is protecting the privacy of student data important?
- What does it take to protect student data privacy?
- How do we ease concerns of parents and other community stakeholders?
- CoSN tools and resources

64% of education IT Leaders said concerns around privacy and security are more important than they were last year.

90% of respondents expect their instructional materials to be at least 50% digital within the next three years.

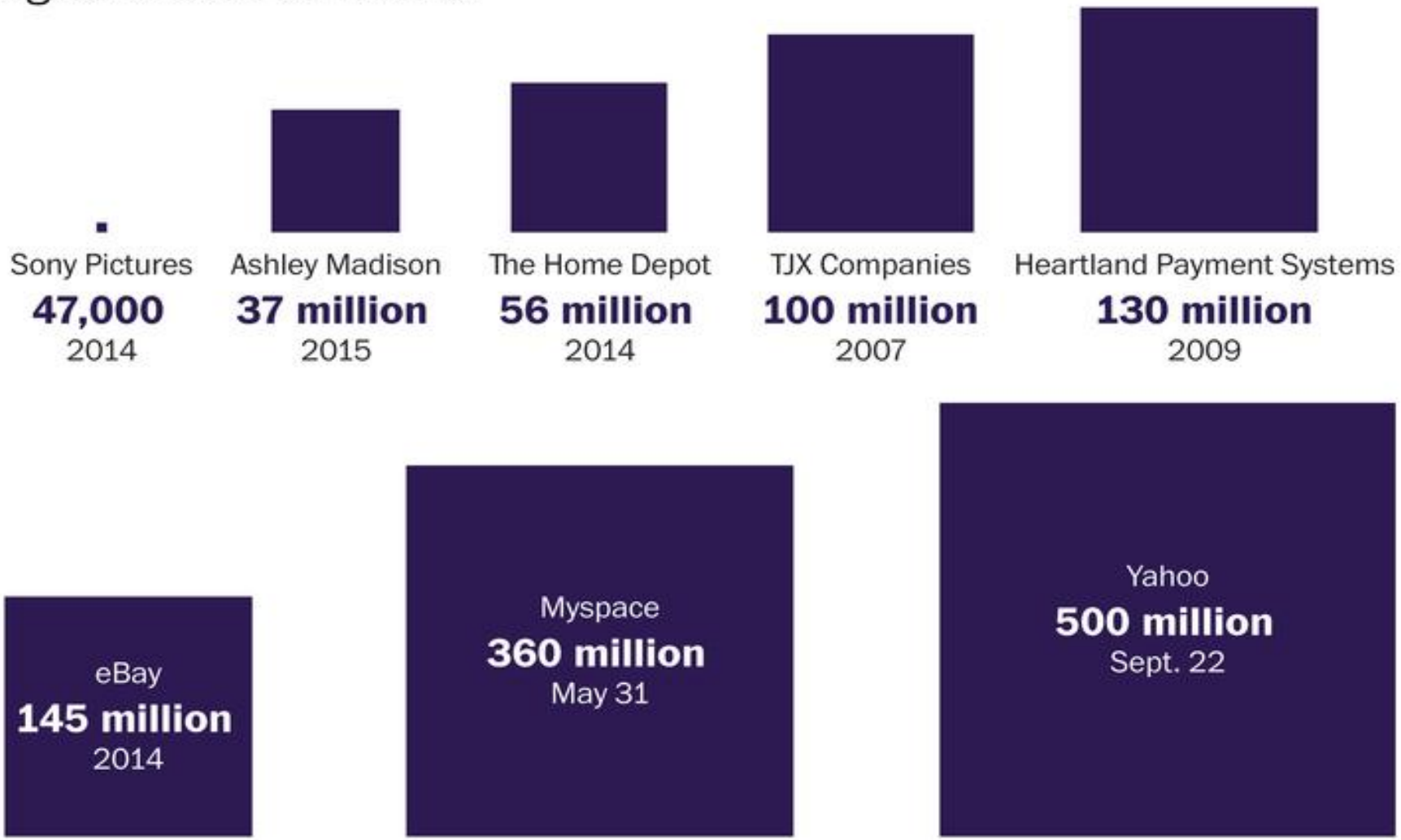
- CoSN 2016 IT Leadership Survey

What's Driving the Concern?

- Security requirements
- Privacy laws
- Third party relationships
- Parents and other community stakeholders

Scaling past data breaches

Yahoo's data breach affected about 500 million accounts, making it the largest breach on record.



Note: Dates are when officials confirmed a data breach occurred.

Sources: Privacy Rights Clearinghouse, news reports

CHRIS ALCANTARA/THE WASHINGTON POST

Security

- ✓ Protecting data from unauthorized access:
  - Human error
  - Hacking
  - Ransomware
  - Malware
  - Lost or stolen equipment

- ✓ Requires costly and complex security infrastructure
  - Specific security expertise
  - Measured against standards
  - Increase protections with increasing sensitivity of the data
  - Constant monitoring, threat mitigation and improvement

Security

- ✓ The time to compromise is almost always days or less, if not minutes or less.

  - 2016 Data Breach Investigations Report (Verizon)

- ✓ “If you’ve got computers and you’re on the web and you’re online, you’re going to have to spend money to protect that.”

  - Wichita School Board Member Lynn Rogers, explaining request for up to $2MM for cybersecurity

http://www.campussafetymagazine.com/article/kan._school_board_looking_for_2m_cybersecurity_improvement/Student_Data

Many school forms require personal and, sometimes, sensitive information…

Your child's personal information is protected by law. Asking schools and other organizations to safeguard your child's information can help minimize your child's risk of identity theft.

- Federal Trade Commission

https://www.consumer.ftc.gov/articles/0040-child-identity-theft

Privacy

- ✓ What data is collected and how it is used and handled:
  - Legal and ethical limitations on collection, use and handling of student personal information
  - Federal and state laws regulate the privacy of student data
  - School systems are responsible for vendor data privacy behavior

- ✓ Requires complex governance framework and enforceable policies and practices:
  - Specific privacy expertise
  - Develop standards aligning with legal requirements and community norms
  - Limit data access
  - Enforce parent rights
  - Exhibit transparency
  - Minimize data collection
  - Regular training, reassessment and improvement

Federal Privacy Laws

- US Department of Education:
  - FERPA (Family Educational Rights & Privacy Act)
  - PPRA (Protection of Pupil Rights Amendment)

- Federal Trade Commission:
  - COPPA (Children's Online Privacy Protection Act)

- US Department of Health & Human Services
  - HIPAA (Health Insurance Portability & Accountability Act)

3 Privacy Laws Simplified

- **FERPA** – Parents have a right to receive a copy of their child's education record and request correction of certain information.
- **PPRA** – Parents have a right to review and opt their child out of surveys involving questions on sensitive subjects.
- **COPPA** – Online service providers must obtain verifiable parental consent before collecting personal information from children under 13.

National Cyber Security Alliance: *Perceptions of Privacy Online and in the Digitally Connected World*

87% of individuals concerned their data is shared without their knowledge/consent.

66% of Americans would accept less personalized content/fewer discounts to keep their personal information private.

Health insurance providers and banking/investment companies **most trusted entities**, yet only were rated at 56 and 57 respectively (out of 100).

Early adopters of technology are generally more **trusting** of all entities.

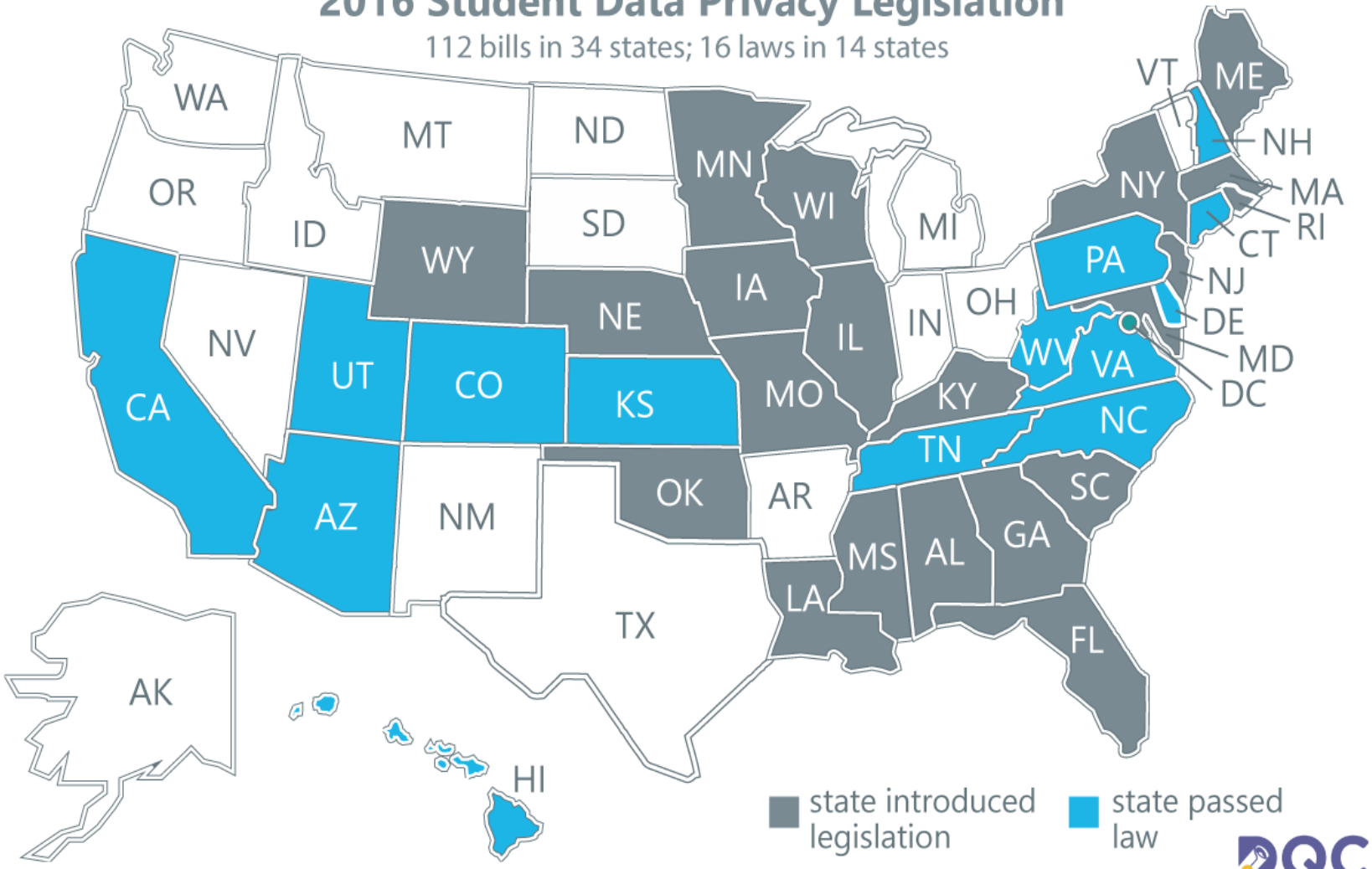
Attitudes About Privacy

Benenson Strategy Group - 800 telephone interviews with registered voters nationwide for Common Sense Media Student Privacy Survey

- Overwhelmingly adults said:
  - Are concerned how private companies with non–educational interests are able to access and use students' personal information
  - Would support various proposals regulating how student data is used
  - Don't know enough about how their schools currently collect, use, store and destroy students' data, such as social security numbers, grades, behavior, and attendance records.
- 86% of adults said “Protecting children's safety and personal information should be priority number one.

2016 Student Data Privacy Legislation

112 bills in 34 states; 16 laws in 14 states

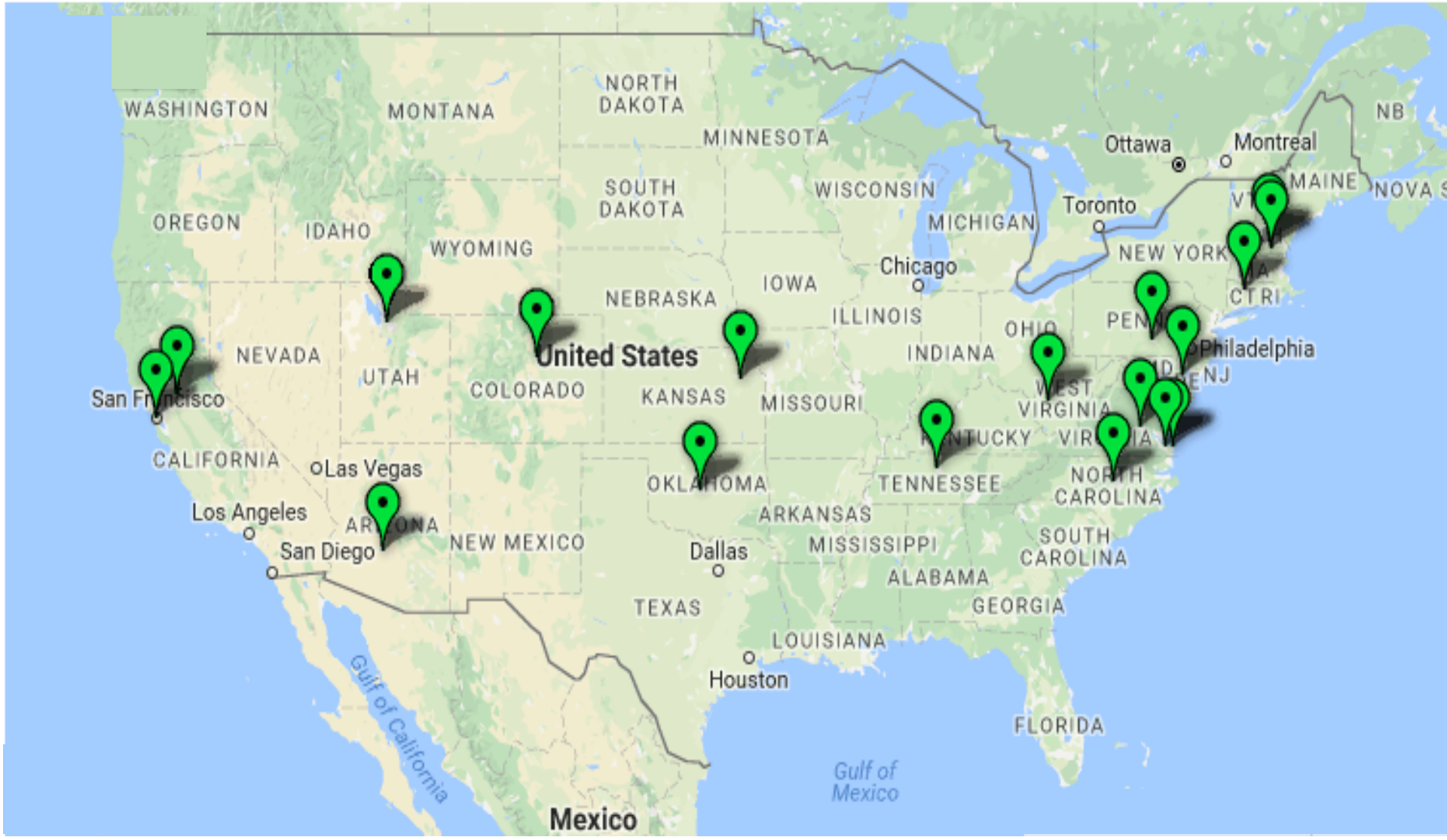


(9/16/16)

DQC
DATA QUALITY CAMPAIGN

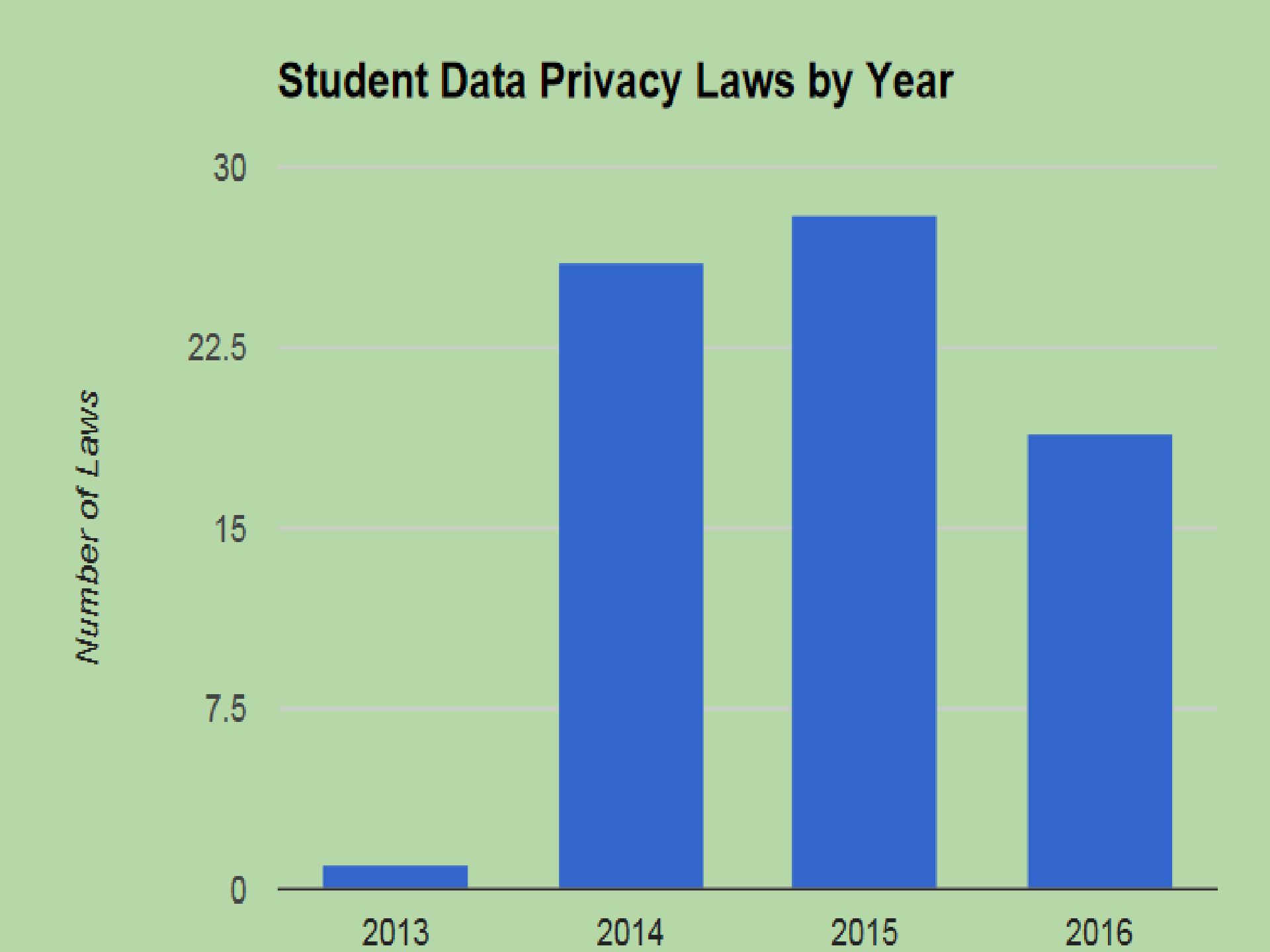
Examining the Student Data Privacy Landscape in 2016

States continue to build on their efforts and introduce laws to protect student data privacy.



Student Data Privacy Landscape in 2016

- ✓ **Student information getting regulatory makeover on massive scale. Legislatures in 38 states considered 185 bills on student data privacy this year. Many with stricter language protections for students, according to policy update report from the National Association of State Boards of Education (NASBE).**
- ✓ **Majority of bills govern online school providers, increase transparency in state & local student data management & add data protection responsibilities to school districts, according to September analysis from Data Quality Campaign**
- ✓ **Lawmakers in 15 states approved 19 bills this year, slightly down from a high of 28 in 2015.**
- ✓ **With the exception of Vermont, every state and District of Columbia has at least introduced student data privacy legislation. Three states — Arizona, Hawaii and Pennsylvania — passed first law on the topic this year - Data Quality Campaign's analysis.**


Student Data Privacy Laws by Year
30
22.5
15
7.5
0
Number of Laws
2013
2014
2015
2016

Data Quality Campaign

Student Data Privacy Legislation
A Summary of 2016 State Legislation

https://tinyurl.com/studentdata2016

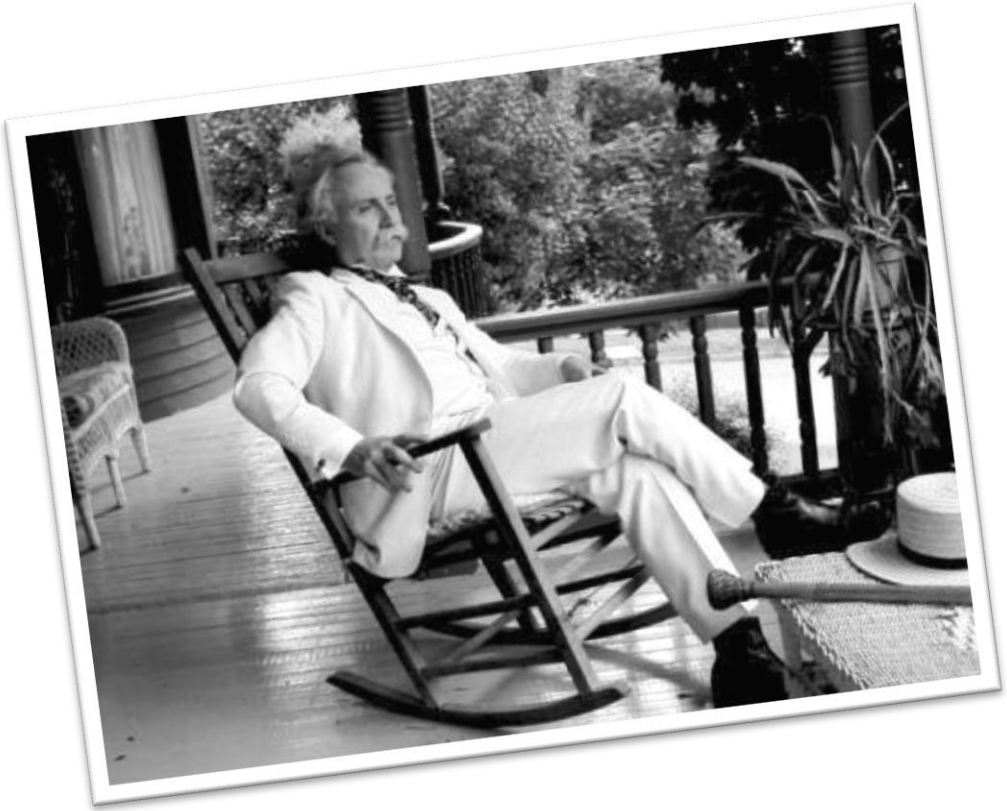
Data Quality Campaign

Looking Ahead to 2017

What to expect next session?

States will:

- Address the role of third-party service providers.
- Amend existing privacy laws and focus on their unique state contexts.
- Explore student privacy issues beyond the education record.
- Turn attention to ESSA, and the number of bills narrowly focused on privacy will decrease.



Laws control the lesser man...

Right conduct controls the greater one.

- Mark Twain

Parent Concerns

- Lack of understanding of the benefits of technology or how it works
- Fear that schools are not maintaining control over the data
- Concern that vendors have access to too much data
- Questions about why data is collected and how it is protected and managed

Concerns over privacy could threaten the use of technology in schools.

Louisiana Data Privacy Laws

- Required State Department of Education to create an anonymous identifier system by May 1, 2015 that does not use students' Social Security numbers,
- State will no longer be able to access students' names, date and place of birth, Social Security number, mother's maiden name, and other information to use for assessment and accountability purposes.
- Strictest law in the country, the offender faces up to a $10,000 fine or three years in prison, or both – school employees are personally liable.
- Biggest problem school administrators have had is not parents saying 'no,' it's parent's not returning the form. That's an automatic denial."

Louisiana Act 837 - 2014

- Main concern of supporters was the Common Core and InBloom.
- Out of state and secondary sharing – especially commercial sharing.
- Limits on student identifiable data.
- Data security a concern.
- Greatest concern about LDOE data use.
- Legislative author wanted parental permission for any use of data.

Louisiana Act 677 - 2014

- Requires school boards to post information regarding the transfer of students' personally identifiable information (PII) to private entities who provide student and other educational services to the School Board.
- Links on district webpage must identify the entities with whom the board has contracts or relationships, pursuant to which, PII is transferred.

- Website much have the name of each entity, a copy of the written contract or agreement between the School Board and the entity, including an addendum added to address the requirements of ACT 837 of the 2014 Legislative session.

Understand Your Responsibilities

- Protecting the privacy and security of student data is part of every school system's fundamental responsibility to protect students from harm.
- Responsibility for bringing appropriate technology into the school system is yours.

Data: Risks and Rewards

- Customized and adaptive learning
- Operational efficiencies
- Early intervention
- Easier to understand what, when and how students learn

- High-value data
- Costly security breaches
- Rising rates of identity theft in children
- Complex compliance requirements

Privacy Begins With Leadership

A school system cannot successfully protect its students without appropriate and informed leadership setting expectations and championing the efforts.

Contrary to what most people believe, trust is not some soft, illusive quality that you either have or you don't; rather ***trust is a pragmatic, tangible, actionable asset that you can create.***

Stephen M. R. Covey

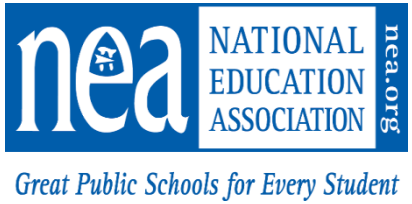
Setting the Stage for Success

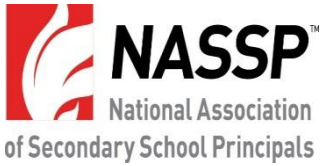
CoSN informs, guides and helps you manage your student data privacy efforts.

Creating the Framework

CoSN and Data Quality Campaign led a coalition of national stakeholders in determining a set of fundamental beliefs for using and protecting student data to guide the work of the education community.

These beliefs are widely shared by the education community





Student Data Principles: How to Use the Data

1. Student data should be used to further support student learning and success.
2. Student data are most powerful when used for continuous improvement and personalizing student learning.
3. Use student data to inform, engage and empower students, families and school system leaders.
4. Provide students, families and educators with timely access to information collected about the student.
5. Use student data to inform and not replace the professional judgment of educators.

Student Data Principles: Working with Technology Providers

6. Share students' personal information only under terms or agreement for legitimate educational purposes; or obtain necessary parent consent. Implement policies to oversee this process.
7. Provide clear, publicly available rules and guidelines for how you and your service providers collect, use, safeguard, and destroy data.
8. Collect and provide access only to the minimum student data required to support student success.

Student Data Principles: Education and Training

9. Everyone who has access to students' personal information should be trained and know how to effectively and ethically use, protect, and secure it.

Student Data Principles: Privacy and Security Framework

10. Have a system of governance that includes:
    - ✓ Rules, procedures, and the individual or group responsible for authorizing data collection, use, access, sharing, and security, and use of online educational programs;
    - ✓ Policy for notification of any misuse or breach of information and available remedies;
    - ✓ Security process that follows widely accepted industry best practices;
    - ✓ Designated place or contact where students and families can go to get informed about their rights your data privacy and security practices.

Anyone who has access to students' personal information should adhere to and build upon these 10 principles.

Stay Updated!

StudentDataPrinciples.Org

Moving Beyond the Framework

Building trust:

- Know your legal and ethical responsibilities
- Take responsibility for bringing appropriate technology into your school system
- Provide proper education and training to students, parents and employees
- Demonstrate your competency around student data privacy and security
- Be transparent with your employees, parents and students
- Continuously examine and improve your governance program

TRUSTED LEARNING ENVIRONMENT

Demonstrating your competence and commitment to student data privacy and security.

Trusted Learning Environment Seal Program

A mark of distinction for school systems, signaling that they have taken specific, measurable steps to help ensure the privacy of student data.

Trusted Learning Environment Program

Created in collaboration with 28 school systems, with support from lead partners…

AASA THE SCHOOL SUPERINTENDENTS ASSOCIATION

ASBO ASSOCIATION OF SCHOOL BUSINESS OFFICIALS INTERNATIONAL

ASCD LEARN. TEACH. LEAD.

Additional partners…

DQC DATA QUALITY CAMPAIGN

iKeepSafe

naesp

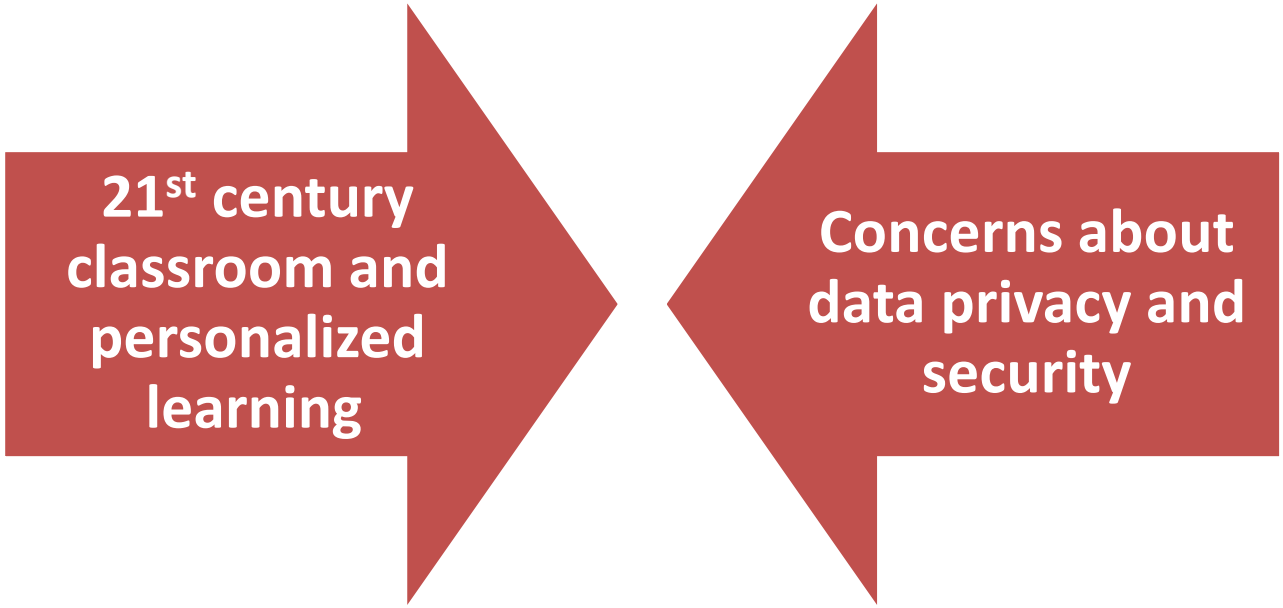
NASSP National Association of Secondary School Principals

NASBE National Association of State Boards of Education

PDK

StriveTogether Every child. Cradle to career.

Why is the TLE Seal Program Important?



How Does the TLE Seal Work?

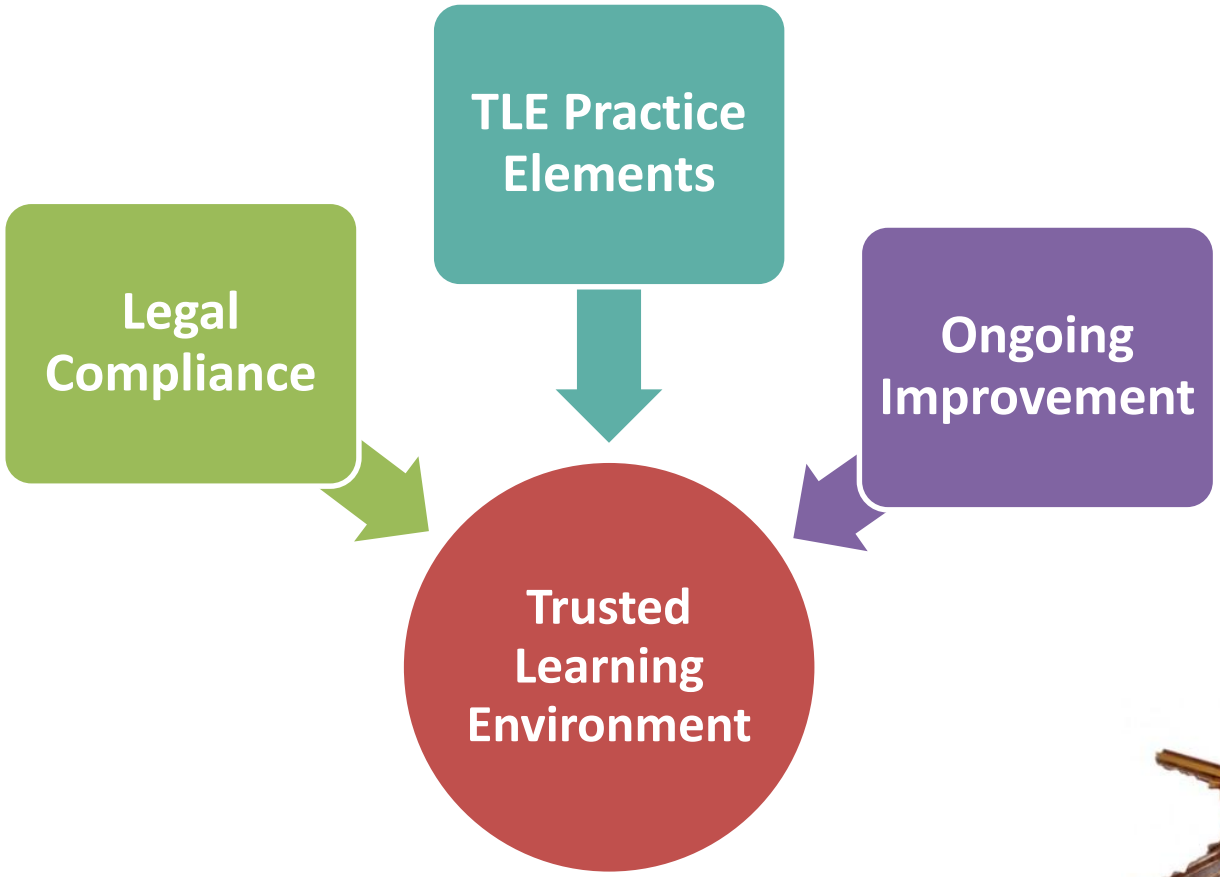
- Evidence
- Application
- Assessment
- Feedback

Open to school systems of all governance structures; public, private, charter and parochial.

Trusted Learning Environment Program Requirements

- ✓Leadership
- ✓ Business
- ✓ Data Security
- ✓ Classroom
- ✓ Professional Development

What Does it Take to Earn the TLE Seal?



What Does Each Practice Entail?

1. **Leadership:** manage and collaborate on use and governance of student data
2. **Business:** establish acquisition vetting processes and contracts to address laws while supporting innovation
3. **Data Security:** audit data privacy and security practices and publicly detail these measures
4. **Professional Development:** conduct privacy and security training, available to all stakeholders
5. **Classroom:** ensure transparency with parents and students while advancing curricular goals

Meaning of TLE Seal

- Demonstrates adherence to publicly available standards around 5 core privacy practice areas.
- Signifies your commitment to student data privacy.

TRUSTED LEARNING ENVIRONMENT

Meet Our TLE Seal Recipients

Butler County (AL) Schools
Cambridge (MA) Public Schools
Denver (CO) Public Schools
Fulton County (GA) Schools
Lewisville (TX) Independent School District
Miami-Dade (FL) County Public Schools
Raytown (MO) Quality Schools

Demonstrating a strong, measurable, public commitment to student data privacy and building trust in their communities.

TRUSTED LEARNING ENVIRONMENT

Build Your Competencies and Trust in Your Community

- Overwhelming positive national and local press celebrating TLE Seal recipients:
  - ✓ 7 Districts Win Trusted Learning Environment Seal for Data Privacy Commitments - Education Dive
  - ✓ Schools Earn National Privacy Designation- eSchool News
  - ✓ TLE Seal of Privacy: Building a 'Trusted Learning Environment' - THE Journal
  - ✓ Small Missouri School District Thinks Big About Privacy and Security - EdScoop
  - ✓ Fulton County Schools Honored for Learning Environment - MDJOnline.com

TRUSTED LEARNING ENVIRONMENT

For More Information and to Apply: TrustedLearning.org

Protecting Privacy in Connected Learning

A CoSN Leadership Initiative

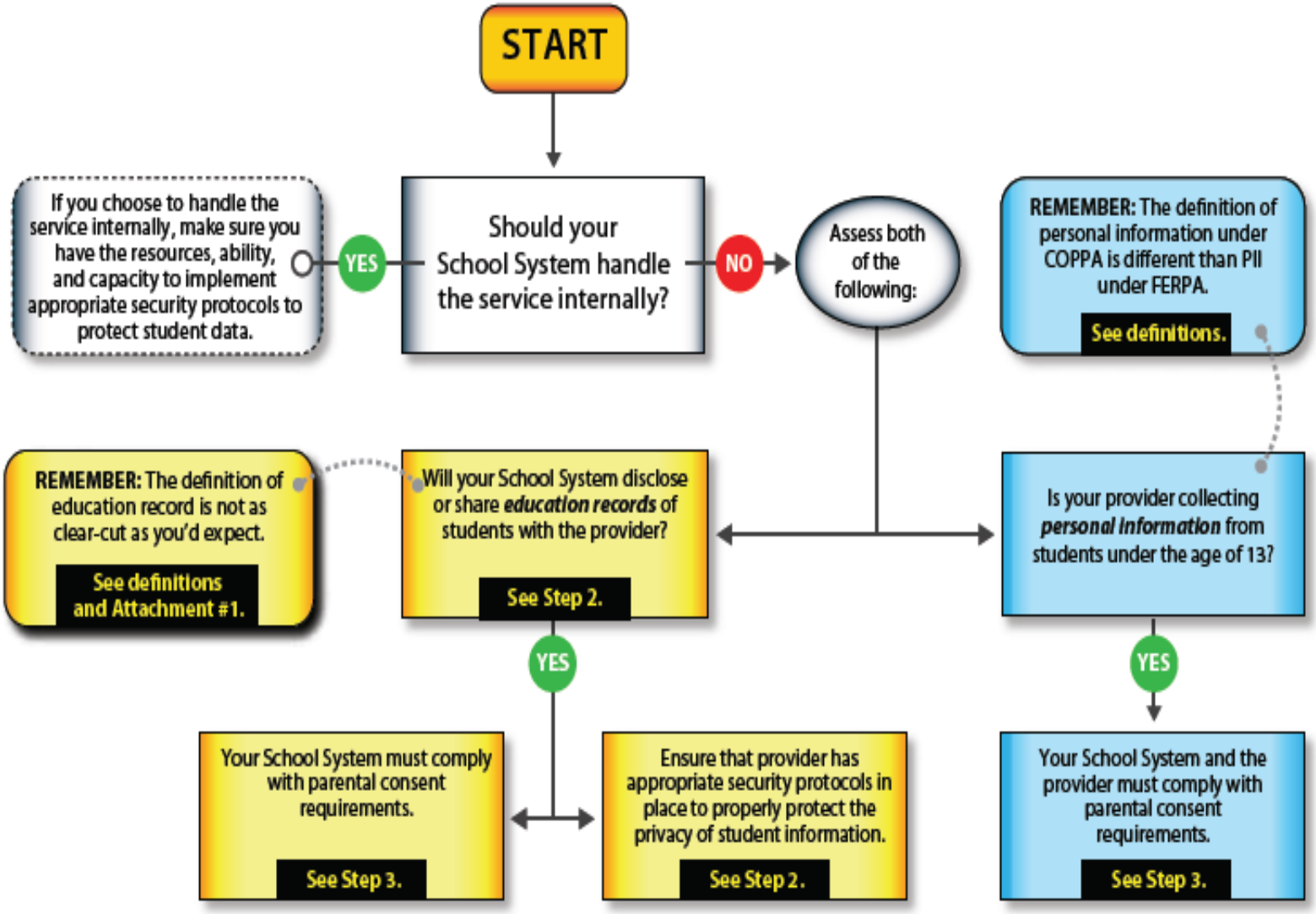
Sponsored by

Microsoft

Mc Graw Hill Education

hp

filewave


START
Should your School System handle the service internally?
YES
If you choose to handle the service internally, make sure you have the resources, ability, and capacity to implement appropriate security protocols to protect student data.
NO
Assess both of the following:
REMEMBER: The definition of personal information under COPPA is different than PII under FERPA.
See definitions.
Is your provider collecting personal information from students under the age of 13?
REMEMBER: The definition of education record is not as clear-cut as you'd expect.
See definitions and Attachment #1.
Will your School System disclose or share education records of students with the provider?
See Step 2.
YES
YES
Your School System must comply with parental consent requirements.
See Step 3.
Ensure that provider has appropriate security protocols in place to properly protect the privacy of student information.
See Step 2.
Your School System and the provider must comply with parental consent requirements.
See Step 3.

Contract Terms

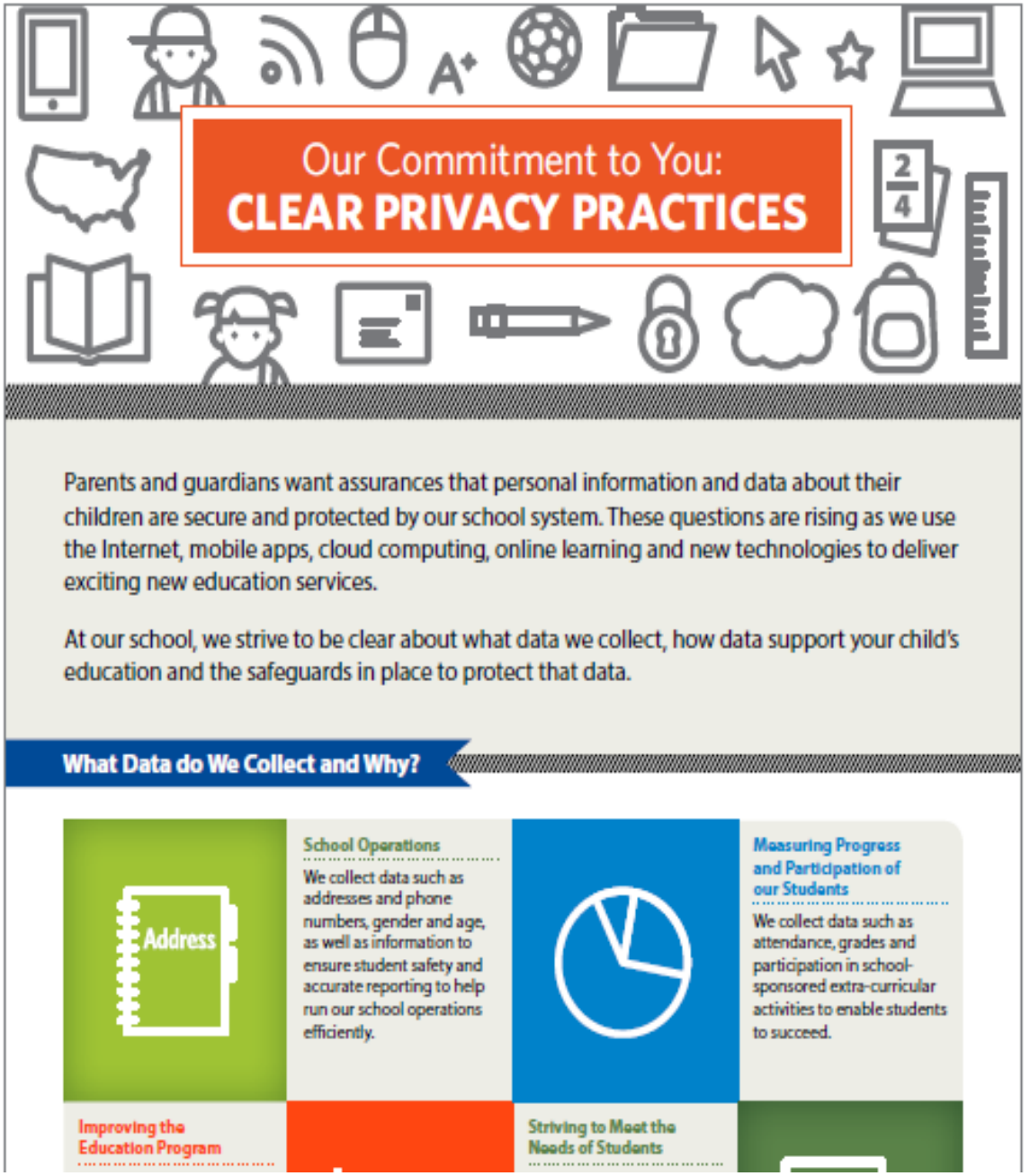
- Contract Scope
- Purpose
- Data Collection, Use and Transmission
- Data Security
- Data Retention and Disposal
- Bankruptcy or Acquisition
- Service Levels and Support
- Governing law and jurisdiction
- Modification, Duration, and Termination Provisions
- Liability

Endorsed by The Association of School Business Officials International

Security Questions to Ask an Online Service Provider

- Data Collection
- Network Operations Center Management and Security
- Data Storage and Data Access
- Data and Metadata Retention
- Development and Change Management Process
- Availability
- Audits and Standards
- Test and Development Environments
- Data Breach, Incident Investigation and Response

Connect with parents: 2-page, customizable infographic available in English & English-Spanish.



Privacy Resources

- CoSN's Protecting Privacy in Connected Learning www.cosn.org/privacy
- Collaborative Effort Led by CoSN & DQC http://studentdataprinciples.org/the- principles/
- Data Quality Campaign www.dataqualitycampaign.org
- Developed by The Future of Privacy Forum www.ferpasherpa.org/-
- Collaborative effort led by the Software & Information Industry Association and The Future of Privacy Forum http://studentprivacypledge.org/
- US Dept. of Education's Privacy Technical Assistance Center ptac.ed.gov
- Sponsored by Intel, *Making Sense of Student Data Privacy*, *Data Security: The First Step to Protecting Student Privacy* and many more resources www.K12BluePrints.com/privacy
- National Cyber Security Alliance StaySafeOnline.org
- US Dept of Ed – Protecting Student Data Training Video https://www.youtube.com/watch?v=deo2F19DK_o
- Common Sense Media http://www.graphite.org/
- Trends in Student Data Privacy Bills in 2016 http://www.nasbe.org/wp-content/uploads/Vance_2016-State-Final.pdf

REGISTER NOW
SAVE $100
HURRY! OFFER ENDS 1/6/17

CoSN2017 INVENT THE FUTURE

CHICAGO, IL • APRIL 3-6, 2017

Who Should Attend?

- Chief Technology Officers
- Directors of Curriculum and IT
- Superintendents
- District Leadership Teams
- Education Service Agencies
- Industry Leaders
- Government Representatives

#CoSN2017

COSNCONFERENCE.ORG

Contact Information

Sheryl Abshire, Ph.D.
@sherylabshire

sheryl.abshire@cpsb.org
Chief Technology Officer – CoSN Board Member
Calcasieu Parish Public Schools
Lake Charles, Louisiana

CoSN
LEADING EDUCATION INNOVATION