Student Data Privacy Q&A

Student Data Privacy Q&A

Jim Siegl joined the Quilt InCommon All Pilots call on Jan. 15, 2015 to share perspectives on Student Data Privacy issues. In advance of that call, some questions had been posted on the email list. Jim provided these answers in an email to the list to help guide the discussion on the call.

Contact Info for Jim:

Jim Siegl, Technology Architect
Department of Information Technology
Fairfax County Public Schools
Jfsiegl1 AT fcps.edu
703-329-7579

Question

1. Which recent breaches of student data privacy provide the most-instructive insights and caveats to regional network operators interested in offering services to k12 based on trusted identity?

Answer

a. E.g. Maricopa County Community College District – 2.4 million records, cost the college $12 million in system repairs, document management and legal fees related to the breach. Two class-action lawsuits have been filed. Employee fired.

Other recent and local-University of Maryland

b. Much of Data Breach in K12 is
  i. Internal
    1. stolen laptop/drive,
    2. Mistaken posting
    3. Student “misbehavior”
  ii. External
    1. (Vendor) Bad Code e.g XSS, BB roster password reset
    2. (Vendor) Error/misconfiguration/migration/update (princeton ftp, LCPS)
    3. External DDOS (start of school year)

(Liability insurance etc. - I would say that the conversation at Educause (CIO forum) is probably more advanced that what I have seen in K12 right now)

The near term focus of fear/concern in K12 seems much more on the collection and use of data of students by vendors (e.g. class dojo) than on data breaches.

Question

2. Which state governments, trade associations or K12 associations are driving the debate and activity on student data privacy? And What in their agenda and activities should we attend to?

Answer

a. Government
  i. Department of Ed Privacy Technical Assistance center (PTAC) – see this essential guidance doc - Protecting Student Privacy While Using Online Educational Services
  ii. FTC COPPA FAQ --see section M for school rules/guidance
  iii. States (subjectively good examples Calif., New York, Oklahoma)

    1. Overall major trends --biometric, parents bill of rights, restriction of commercial use of data, CPO, requirement to post data element inventory, some technical requirements (encryption)

  iv. UK Gov Checklist for Educational Cloud services

b. Industry / Trade and Professional Associations
  i. CoSN (privacy Toolkit)
  ii. SIIA (Analysis of state Ed Privacy Laws)
  iii. IAPP (Good resources in the CIPT technical certification)
  iv. Toy Industry Association (COPPA Checklist for Mobile Apps)

c. Advocacy Groups and “Think Tanks”
  i. Data Quality Campaign
  ii. Common Sense Media (e.g. Graphite.org)
  iii. iKeep Safe
  iv. Harvard Berkman Center Student Privacy Initiative – publishes weekly summary of news, good whitepaper “straw man” analysis of a hypothetical service
  v. Future of Privacy Forum (Ferpa Sherpa)

Question

3. Many school districts provide student identities for multiple purposes via both Student Information Systems (e.g., Infinite Campus), social/cloud-based providers (e.g., Google Apps for Education) and individual academic software-as-a-service providers. How will the collision/collusion/confusion among and about these providers on student data privacy affect how regional network operators develop and deliver trusted identity services to K12?

Answer

i. Confusion-Sign in with Google ID – Many K12 educators in my district think that “sign in” with Google means that the site does not create a “local” account for the student
ii. Collusionesque -Slippery Slope (Google ID) - Many Google OAuth2 enabled services do not present terms or privacy policies when “installed” thru the google drive, docs. Or sheets web application interface
iii. Collision –
    1. Where the meaning / rights / role of an account is different in one context vs another – the meaning of “parent” is a good example (educational rights, enrolling, custodial, etc..)
    2. another is where a setting in an Account provider (like google apps for EDU) conflicts, breaks a function in a service provider (the consumer google service MyMaps)

Question

4. To retain the trust of our K12 members and customers regarding student data privacy, what are the three most-important best practices to make our standard operating practices?

Answer

a. Usable Transparency
    i. CUPS (what is collected, used, protected, shared), Point of Contact/Data Steward, retention, destruction
b. Notice and Choice
    i. Access and correct information (key to anything that is ED record)
c. Think about privacy, security and safety