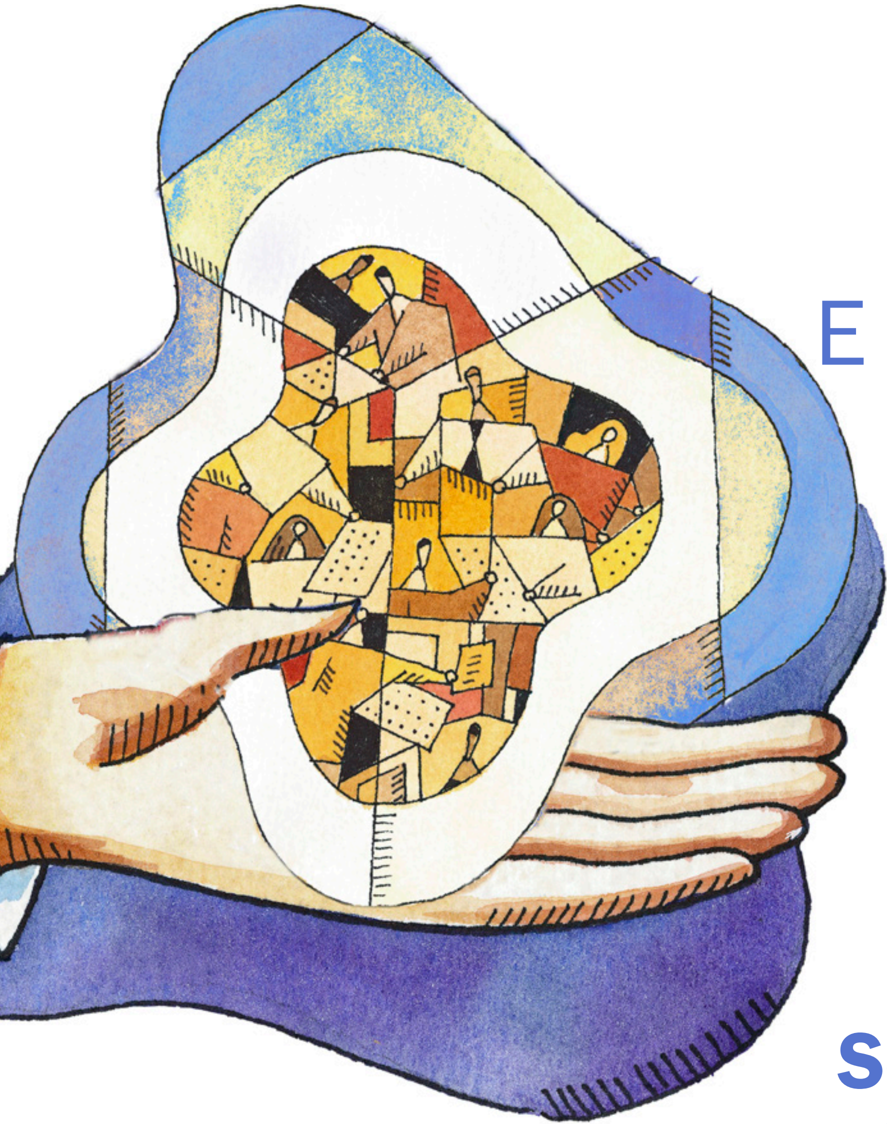
CoSN Member Only
Winter 2013



EDTECHNEXT
Emerging technology for K–12 education

Security and Privacy of Cloud Computing

In classes across the country, students are learning in the cloud. In school, at home, wherever they are, students are using online textbooks, watching videos, exchanging emails, collaborating on documents, storing files, editing photos and more.

Cloud computing has moved from an emerging technology and into the mainstream, with nearly 90 percent of K–12 institutions reporting using one or more cloud-based applications (O'Keeffe & Co., 2011). But as school districts expand the classroom beyond their walls, there are additional privacy and security impacts.

This report deals primarily with the privacy, security and regulatory compliance impact of "Software-as-a-Service" (SaaS) cloud computing. For an overview of the different types of cloud computing, see the CoSN *EdTechNext* Winter 2009 report, "Cloud Computing: A Billowing Virtual Infrastructure for Services—and Savings."

Defining Terms

Security deals with the "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved" (Pearson, 2012; ISO, 2005).

Privacy is the "assured, proper, and consistent collection, processing, communication, use and disposition of personal

ADVANCING K-12 TECHNOLOGY LEADERSHIP
www.cosn.org

information (PI) and personally identifiable information (PII) throughout its life cycle" (Hogan, Liu, Sokol & Tong, 2011).

Fears, Risks and Realities

When schools store data in programs hosted "in the cloud," they lose a degree of control over the information. While security and privacy concerns are not unique to cloud computing, the important distinction between on on-site applications and SaaS is that information is stored on the public Internet, managed by others and sometimes resides on shared servers. Here are some common security and privacy risks associated with cloud computing and how to manage them:

- **Data breach** due to unpatched or improperly configured servers, malware or SQL injection, cross-site scripting or other software bugs. Unlike on-premise software, schools do not control the updates and patches of cloud computing software. Companies including Dropbox, Google and others have had incidents where a software bug has exposed user data. Precaution: See "Securing Data in the Cloud" and "Cloud Contract Considerations," below, for more details.
- **Data loss (or leakage)** by users who unknowingly (or intentionally) expose information by sharing or sending information. While this also can happen with internal systems, the fact that cloud computing applications are typically available on the Internet increases the potential exposure exponentially. Precaution: Policies and user education and training are key to reducing this risk. Software called data loss prevention tools can scan systems and audit permissions, checking for data that fits certain patterns (e.g., Social Security or credit card number).
- **Password reuse.** The average user maintains 25 separate website accounts but uses just 6.5 passwords (Florencio & Herley, 2007). If a site has a data breach or leak, or if someone gets hold of a username and password written on a sticky note, anyone who uses the same password on multiple sites is at much greater risk. Precaution: Using two-factor authentication–such as using a text sent to a cell phone in addition to a password, having different strong passwords for each site and using a "password vault" tool that securely creates and stores strong passwords—or federated authentication can reduce this risk. For more information on federated authentication, see the COSN report *Single Sign-On, Multiple Benefits.*
- **Collection and aggregation of personally identifiable data.** Some cloud providers allow advertisements to be served to students even for "contracted" (not consumer) services in the school setting. Precaution: Most web browsers support third-party plug-ins that block many of the techniques such as "cookies" that ad networks use to collect data for user tracking and profiling. For more on this topic, see "Privacy" and "[Please] Do Not Track," below.

Privacy Fast Facts

- **81 percent** of parents of online teens say they are concerned about how much information advertisers can learn about their child's online behavior.
- **69 percent** of parents of online teens are concerned about how their child's online activity might affect their future academic or employment opportunities.
- **69 percent** of parents of online teens are concerned about how their child manages his or her reputation online.

Source: Madden et al., 2012. *Parents, Teens, and Online Privacy.* Pew Research Center's Internet & American Life Project.

A recent survey of 151 IT government managers found that nearly three-quarters consider the security of cloud computing a major worry (MeriTalk, 2012), but how does that concern bear out in reality?

A study by Alert Logic examined more than 60,000 security incidents for both on-premise system and cloud computing environments. This study concluded that, while the nature of the threats is different in the two environments, when looked at as a whole, the total risk was similar and neither environment is less secure.

Many forms of cloud computing are, at their root, a type of outsourcing. Schools often outsource certain functions, from payroll to transportation. Given schools' scarce resources and the complexity and rapidly increasing pace of security threats, companies that specialize in cloud computing services are able to offer better security, especially for smaller districts, than a comparable on-premise solution.

> **"There is simply no example where a (school) can outsource its services to a provider … and not be on the hook for compliance. Service providers enable compliance but the institution is ultimately on the hook to achieve, maintain and prove it."**
>
> **— Brett Emmerton, Director, Global Education & Research Platform Solutions at Dell Services**

Securing Data in the Cloud

Securing data in the cloud requires securing data in two ways—when it is in "in transit," or being transmitted between the user and the cloud, and when it is "at rest," or stored in the cloud, typically in a database or file system.

Data in transit typically is secured through the use of SSL certificates to encrypt communications. It is important to consider whether all traffic on a website is encrypted, or only traffic on the registration and login pages. If all traffic is not encrypted, the site may be vulnerable to session hijacking when the site is used over unencrypted Wi-Fi and wired networks. This can occur if an unauthorized user impersonates the legitimate user.

Data at rest is secured by encryption or "hashing" the data where it resides. Encryption is a (two-way) function. It is reversible; a mangled string of data can by decrypted with a key to get the original string. Passwords should be hashed, which is the transformation of a string of characters into a shorter set of characters or a key that represents the original data. Hashing is a one-way function, meaning it cannot be reversed. Most cloud services for schools do not provide for encryption of data at rest—or they require the use of third-party add-on products. However, encryption at rest is a valuable feature, provided that the school alone controls the encryption. This protects against the threat of unauthorized access to student personal information by cloud provider staff or by a hacker.

Many websites that schools use allow the batch (or bulk) creation of student accounts by uploading spreadsheets of student data. It is important to secure the transfer, via https (Hyper Text Transfer Protocol with Secure Sockets Layer, or SSL) or SFTP (Secure File Transfer Protocol) and storage of this data.

Student IDs as Username

It is a common practice when creating accounts for cloud-based services to use student IDs as the usernames. If a student ID is used as a username, it should be declared as "directory" information.

“Contracted” vs. Consumer Cloud Computing

One critical distinction when evaluating security, privacy and compliance is the difference between contracted vs. “consumer” cloud applications. Jim Siegl, a technology architect for Fairfax County (VA) Public Schools, explains this difference among several common tools:

“In cloud applications (SaaS) like Google Apps for Education and Microsoft Office 365, there is a contract between the provider and the school district that covers security, privacy, FERPA [Family Educational Rights and Privacy Act] and COPPA [Children’s Online Privacy Protection Act] and provides certain assurances and responsibilities for both parties. By contrast, Gmail and Hotmail are ‘consumer’ services. These services have nearly all of the same features as the email in the contracted products, but the agreement is between the end user and the provider. The school is not a party to this relationship and has no rights, and no ability to investigate or assurances as to how the provider handles data.”

Contracted cloud computing products can be free or fee-based. Many offer the ability to configure access, such as allowing email only within the school system or grade level.

“Configuration is key and should be investigated to make cloud computing options age-appropriate, while still allowing students the opportunities to create,” says Donna Williamson, technology coordinator at Mountain Brooks Schools in Alabama.

[Please] Do Not Track

Unlike the “do not call” registry, the Do Not Track proposal is a two-step process. First, Do Not Track includes a machine-readable header sent by your browser every time you visit a web page indicating that you don’t want to be tracked (EFF, 2012). Second, it is up to each website what to do with that information including what is meant by “tracking.” The Do Not Track system is voluntary, and there are no legal or technological requirements for its use (W3C, 2012). As of late 2012 recent versions of most major browsers all support sending the Do Not Track header; however, very few websites have implemented processing of the Do Not Track header.

Cloud Contract Considerations

In light of potential privacy and security risks, it’s important to carefully evaluate cloud vendor offerings. A service level agreement (SLA) should include as many of these considerations as possible:

Availability

- Does the provider offer a guaranteed service level?
- What is the backup-and-restore process in case of a disaster?
- What is the provider’s protection against denial-of-service attack?
- What happens to your data if the provider shuts down or is sold?

Security

- Does the provider use SSL encryptions on all pages, and not just the login and account creation pages?
- For multi-tenant hosting (many schools sharing the same system), how is data separated from that of other customers?
- Does the provider perform internal and external penetration testing, vulnerability testing and intrusion prevention?
- Does the provider perform background checks on personnel with administrative access to servers, applications and customer data?
- What is the provider’s process for creating accounts and resetting passwords? Can this process be automated and is it available outside of school hours?

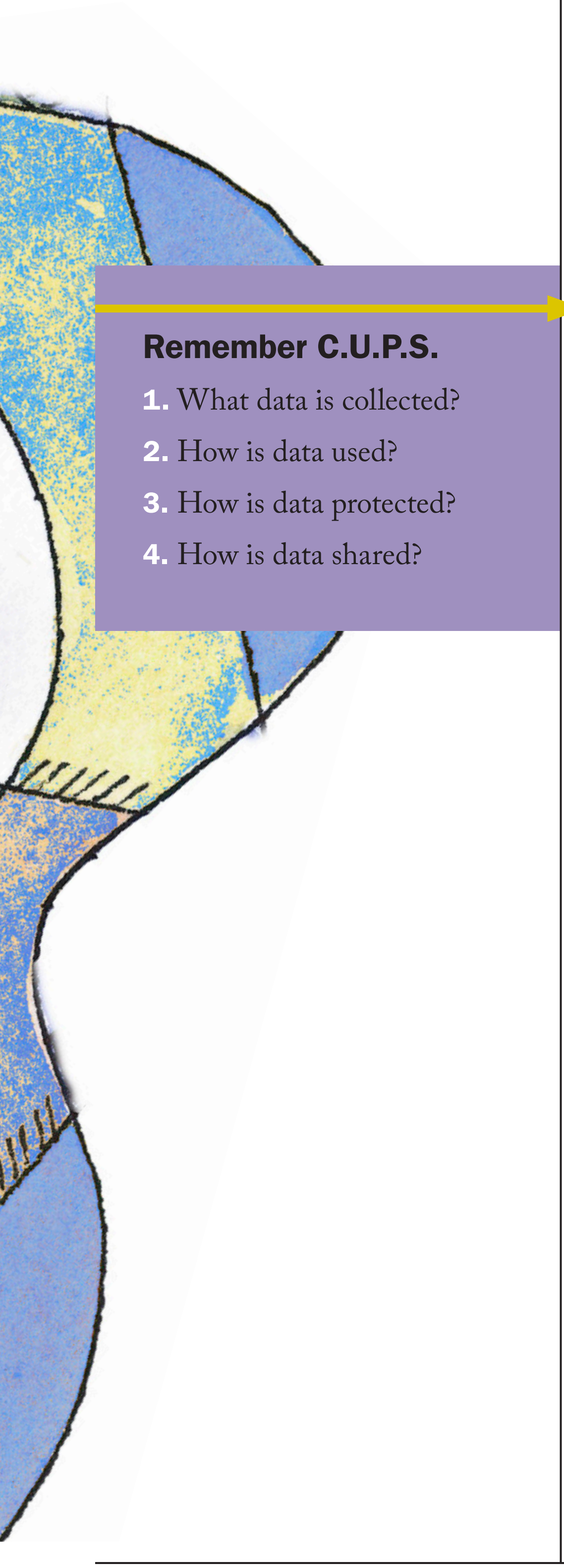
- What is the provider's process (and audit procedures) for network security to ensure that customers will not compromise the provider's infrastructure?
- What are the provider's procedures for configuration management, patch installation and change management for all servers and PCs involved in delivery of contracted services?
- What happens if your cloud service provider has a data breach?
- Do you have the ability to perform security incident investigations or e-discovery? If not, will the provider assist you?

Legal and Regulatory

- Where is data hosted?
- If there is a contract, does it state the provider (and any subcontractors) will operate as a "School Official" as defined by FERPA?

Privacy

Reading the privacy policies of all of the websites used in a year by the average web user would take an estimated 244 hours (McDonald & Cranor, 2008). To make that job easier, remember the acronym C.U.P.S for the four things to look for:



Remember C.U.P.S.

1. What data is collected?
2. How is data used?
3. How is data protected?
4. How is data shared?

Collection. First, the privacy policy should state what information the website can gather from the user, personally identifiable and anonymous, directly and indirectly:

- What personal information is collected?
- How is that information collected (e.g., forms, logs, cookies, tracking pixels)?
- What data do other companies on the website collect?
- What privacy controls are offered to the user?
- Are the website's privacy practices certified and audited by a trusted third party (e.g., TRUSTe, BBBOnLine or WebTrust)?

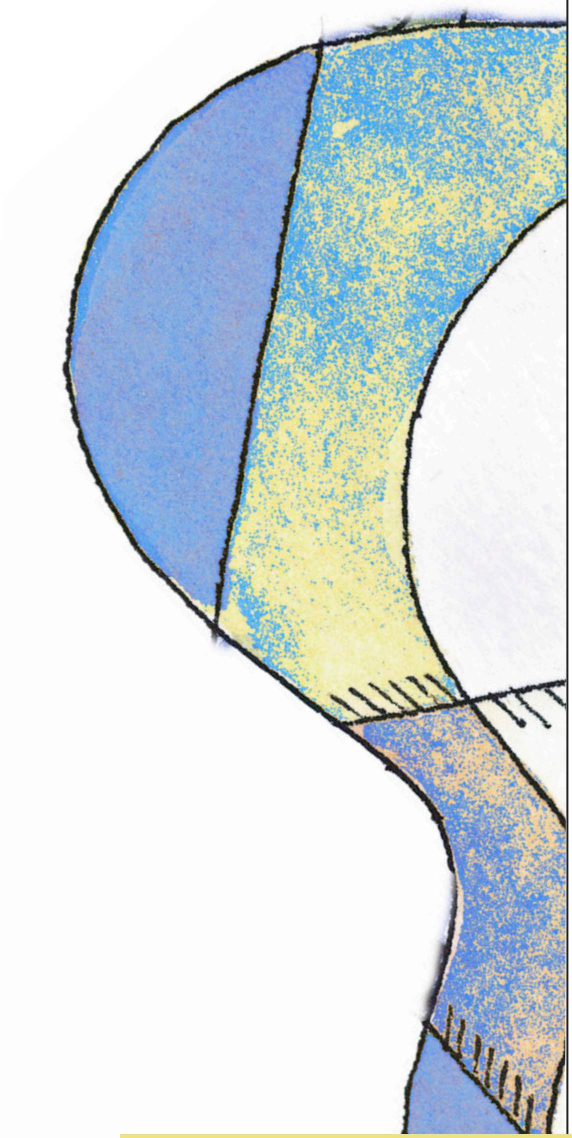
Use. Second, the privacy policy must reveal the information gathered, and show how it handles that information:

- How will the information be used?
- How does the site use the information?
- How long will information be kept?
- Who owns the data?
- Can the data be exported?

Protection. Third, the privacy policy should describe how information is protected:

- Who has access to the data?
- How will it be transmitted and stored?
- What happens if the provider has a data breach?

Sharing. Fourth, the policy should be clear about what information is shared with third parties, including advertisers and tracking networks.



Cloud Computing, Privacy and the Law

COPPA

The Children's Online Privacy Protection Act (COPPA) affects websites that knowingly collect information about or target children under the age of 13. It details what a website operator must include in a privacy policy, when to seek verifiable consent from a parent or guardian, and an operator's responsibilities to protect children's privacy and safety online, including restrictions on marketing to those under 13 (FTC, 2012).

Recent Changes to COPPA. A December 2012 update to COPPA expanded the definition of personally identifiable information to include geolocation data, photos, videos and audio files that contain a child's image or voice, and "persistent identifiers" (tracking cookies) that could be used to build a profile over time and across different websites or online services. The update applies to mobile apps and third-party website "plug-ins" (e.g., advertising networks), as well as websites, and permits online services designed for both children and a broader audience to comply with COPPA without treating all users as children. The changes take effect July 1, 2013 (FTC, 2012).

Parental Consent and Schools. Because of the appeal of free, educational cloud computing tools, understanding "the [COPPA] limitations to online apps for children under 13 … is a BIG issue with limited budgets,“ says Ouida Myers, North Carolina Department of Public Instruction. COPPA allows, but does not require, schools to act as agents for parents in providing consent for the online collection of students' personal information. For example, schools may use their acceptable use policy (AUP) to inform parents of the online services that are provided to students or they may choose to collect parental permission for individual websites (FTC, 2012).

COPPA does not apply to "school districts that contract with websites to offer online programs solely for the benefit of their students. For example, a school or district might contract with a web-based testing service, a provider of a learning management system or online gradebook (FTC 2008).

One School's Approach to COPPA. Montclair Kimberley Academy, a pre-K–12 independent school in Montclair, NJ, provides a letter to parents as part of its admissions contract. The letter describes the broad parental consent and provides a link to a school webpage with a list of third-party computer applications and web-based services the school plans to use, with links to their privacy policies and terms of service: http://www.mka.org/page.cfm?p=810

On his blog, William Stites, director of technology at the academy, offers a sample letter for schools to adapt, with guidance from their administration and attorneys: http://www.williamstites.net/2012/05/22coppa-and-verifiable-parental-consent/

Terms and Conditions May Apply. Even if a site does not fall under COPPA, the site's terms and conditions may prevent someone under 13 from using the site. Schools might need to address scenarios like these in their security and privacy planning:

- Sites that do not fall under COPPA but do not permit users under 13
- Sites that fall under COPPA but have a contract with the school district (e.g., Google Apps)
- Sites fall under COPPA, but the school acts as parental agent under COPPA FAQ 55 (e.g., Evernote)
- Sites that do not fall under COPPA and allow users under 13 with parental permission, or with the school acting as parental agent. Khan Academy, a nonprofit, falls into this category.
- Sites that do not fall under COPPA and only allow users under 13 if the parent creates the account (e.g., Apple iTunes)

FERPA

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

However, FERPA allows schools to disclose those records, without consent, to school officials with legitimate educational interest. Schools may share basic "directory" information, such as student names and addresses, if they give parents the opportunity to opt out. However, written permission is required to release all other student-level information if it is linked to any information that would enable a member of the school community to identify the student (U.S. Department of Education, 2012).

FERPA does not prohibit the use of cloud computing, but it provides conditions for which a school can outsource to a cloud provider under the "school official" exception. Specifically, the outside party must:

- perform an institutional service for which the school would otherwise use employees;
- be under the direct control of the school with respect to the use and maintenance of education records; and
- be subject to requirements governing the use of personally identifiable information from education records (U.S. Department of Education, 2011).

Privacy, Security and Mobile Devices

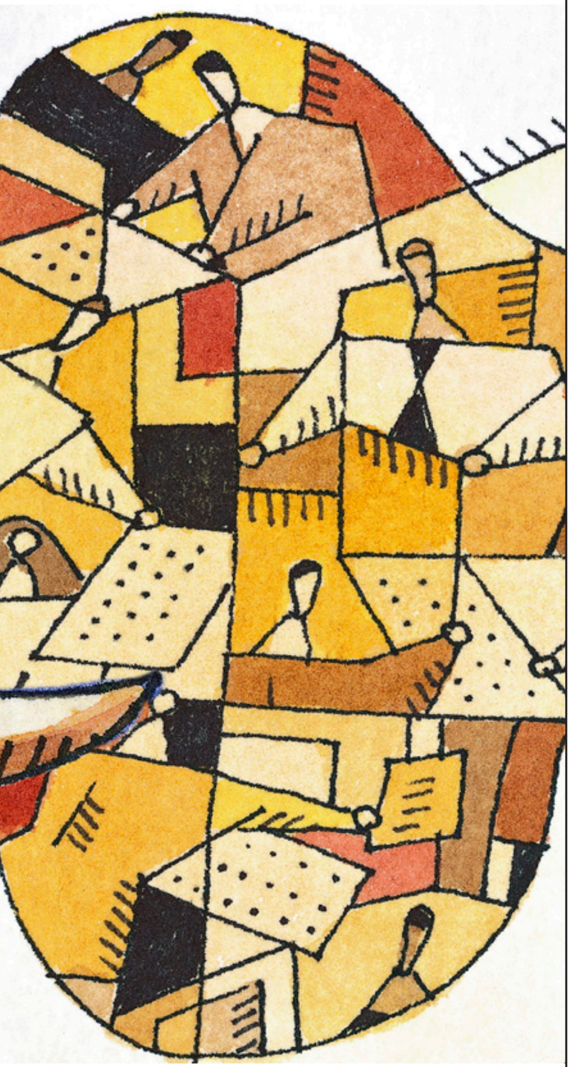
Many of the hundreds of thousands of mobile "apps" are really just front-end clients to cloud computing services. These apps carry security and privacy concerns unique to mobile, include location tracking, advertising networks, and the ability to upload and post users' contact data to other cloud services, such as Twitter and Facebook, on the users' behalf. While recent changes to COPPA provide some regulation for children under 13, the privacy of mobile apps is a concern for users of all ages.

> **"The limitations to online apps for children under 13 … is a BIG issue with limited budgets and free apps that are restricted [under COPPA]."**
>
> ***— Ouida Myers, North Carolina Department of Public Instruction***

When evaluating mobile apps, schools should examine what information is transferred from the mobile device to the cloud. For Android apps, this information is typically described in the Google Play store description of the app; similar information is available for some iOS apps (cluefulapp.com) and websites (apps.secure.me).

Communicating about Security and Privacy in Cloud Computing

There is no combination of technology, policies or SLAs that can completely eliminate all of the security and privacy risk of cloud computing. Education for students in acceptable and responsible use of technology, professional development for staff, and clear and transparent communication with parents on how their child's privacy is being secured are essential to minimizing the real and potential privacy and security risks of cloud computing.



References and Resources

The Privacy Technical Assistance Center (PTAC)

The U.S. Department of Education has established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality and security practices related to student-level longitudinal data systems. Resources include a data sharing agreement, data privacy and security governance checklists, security best practices, and a model notification of rights. ptac.ed.gov

CoSN Leadership Initiative: Cyber Security for the Digital District: Tools and Resources. http://www.cosn.org/Initiatives/CyberSecurity/CyberSecurityInformation/ToolsandResources/tabid/5262/Default.aspx

CoSN. Cloud Computing Resources. http://www.cosn.org/ETNCloudComputingResources/tabid/5749/Default.aspx

Alert Logic (2012). *An Empirical Analysis of Real World Threats: State of Cloud Security Report.* http://www.alertlogic.com/wp-content/uploads/alert-logic-fall2012-cloud-security-DIGITAL.pdf

Apple (2008). Application-Based Services Terms of Use. http://www.apple.com/internetservices/terms/membership_terms.html

Cloud Security Alliance (CSA). (2011). S*ecurity Guidance for Critical Areas of Focus in Cloud Computing V3.0.* https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

CSA. (2010). *Top Threats to Cloud Computing V1.0.* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Delaney, M. (April 5, 2012). "13 Questions Every District Should Ask Its Cloud Vendor." *EdTech* Magazine. http://www.edtechmagazine.com/k12/article/2012/04/13-questions-every-district-should-ask-its-cloud-vendor

Electronic Frontier Foundation (EFF). (2012). "Do Not Track." https://www.eff.org/issues/do-not-track

CoSN appreciates the support of these EdTechNext sponsors:

Adobe

Comcast

Gartner

Hewlett–Packard

Houghton Mifflin Harcourt

Kajeet

Lenovo

Lightspeed Systems

Pearson

Pearson Foundation

Qualcomm

SAFARI Montage

SchoolDude

SmartTechnologies

Steelcase

Wireless Generation

COSN'S EMERGING TECHNOLOGIES

Federal Trade Commission (FTC). (Dec. 19, 2012). "FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Children's Online Privacy Protection Rule." http://www.ftc.gov/opa/2012/12/coppa.shtm

Florencio, D., & Herley, C. (2007). "A Large-Scale Study of Web Password Habits." Association for Computing Machinery: Proceedings of the 16th International Conference on the World Wide Web https://research.microsoft.com/pubs/74164/www2007.pdf

FTC. (2012). *Mobile Apps for Kids: Disclosures Still Not Making the Grade.* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf

FTC. (2008). Frequently Asked Questions about the Children's Online Privacy Protection Rule. http://www.ftc.gov/privacy/coppafaqs.shtm

Hogan, M., Liu, F., Sokol, A., & Tong, J. (2011). *NIST Cloud Computing Standards Roadmap*. National Institute of Standards and Technology (NIST). http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf

International Organization for Standardization (ISO). (2005). *ISO 27001. Information Security Management – Specification with Guidance for Use.*

Madden, M., Cortesi, S., Gasser, U., Lenhart, A., & Duggan, M. (Nov. 14, 2012). *Parents, Teens, and Online Privacy.* Pew Research Center's Internet & American Life Project. http://pewinternet.org/Reports/2012/Teens-and-Privacy.asp

McDonald, A.M., & Cranor, L.F. (2008). "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society 4(3).* http://www.is-journal.org

MeriTalk. (2012). *Mission-Critical Cloud: Ready for the Heavy Lift?* http://www.meritalk.com/pdfs/mission-critical-cloud/MeriTalk_Mission_Critical_Cloud_Press_Release_Final.pdf

O'Keeffe & Co. (2012). CDW Cloud Computing Tracking Poll. http://www.okco.com/our-work/projects/cdw-cloud

Pearson, S. (2012). *Privacy, Security and Trust in Cloud Computing.* HP Laboratories. http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf

Privacy Rights Clearinghouse, (2012). Online Privacy: Using the Internet Safely. https://www.privacyrights.org/fs/fs18-cyb.htm

Siegl, J. (2012). Privacy, Audit and Advertisements in Google Apps for Education. https://docs.google.com/spreadsheet/ccc?key=0AggHIMys1Nn8dEhwUm9JSUFlNmdSc29ZVFhXWGdSRnc

U.S. Department of Education. (Dec. 2, 2011). "Family Educational Rights and Privacy, Final Rule." *Federal Register* 76(232). www.gpo.gov/fdsys/pkg/FR-2011-12-02/html/2011-30683.htm

U.S. Department of Education. (2012). Frequently Asked Questions—Cloud Computing. http://ptac.ed.gov/sites/default/files/cloud-computing.pdf

World Wide Web Consortium (W3C). (Nov. 26–27, 2012). W3C Workshop: Do Not Track and Beyond. http://www.w3.org/2012/dnt-ws/papers.html