2015 COSA School Law Practice Seminar

Advising School Districts in Cloud Computing Contracts

Tom Tokarz, Special Counsel, Henrico County Public Schools, VA

Copyright © 2015 National School Boards Association. All rights reserved.

Some basics about cloud computing

- You have been using cloud computing for years
- Cloud computing: use of software stored on third party servers and storage of data in third party data centers
- Fordham study: 95% of school districts use cloud computing

Basics about cloud computing for schools

- Software as a Service (SaaS): vendor provides online access to software and stores data
- Examples: Office 365, Adobe Creative Cloud, MUNIS, School Dude, and Pearson PowerSchool
- Infrastructure as a Service (IaaS): third party acts as an online data repository
- Significant vendors: Amazon Web Services, Microsoft, Google, and IBM

Why do schools use cloud computing?

- Some software only available in cloud
- Frees IT department from updating servers and user computers
- Allows use of mobile devices and access from anywhere
- Storage economies of scale
- Easy scalability and data backup and recovery

Specific risks with cloud computing

- Configuration or maintenance errors of service provider
- Service provider's storage of data for multiple users without necessary safeguards
- Bankruptcy, business failure, downtime of service providers
- Lack of leverage to get specific protections for school district
- Service providers give bigger target for hacking or other data breaches

More specific risks with cloud computing

- Poor vendor or school district security practices
- Teachers and principals signing up without procurement, IT, or legal approval
- Improperly configured or poorly updated school district equipment and software
- Access through unsecured devices, *e.g.*, smartphones, tablets, especially by teachers and students

Near universal truths about IT contracts

- The vendor almost always oversells the product.
- The IT department almost always underestimates the problems.
- The implementation schedule almost always slips.
- Teachers and principals sign IT contracts without worrying about procurement laws or legal review.
- Users don’t know or follow the contract terms.

Before negotiations begin

- Participate, if possible, in the procurement process.
- Specify contract terms in the request for proposals.
- For large or mission critical contracts, attend the initial vendor presentations and negotiations.
- When obtaining best and final offers, provide guidance for issues that need clarification.
- Identify problematic provisions in the terms and conditions of cooperative procurement contracts.

Questions to ask potential vendors

- Will school district data have to be converted?
- Are any new program interfaces required?
- How will school district personnel be trained?
- What data audit trails are provided?
- How do you handle litigation holds?
- What is required for the school district to get a complete copy of its data on demand?
- What are your internal security measures? How do you separate applications and data from different clients?
- What are your incident response procedures?

More questions to ask potential vendors

- What happens to your software and our data if you go out of business? Do you maintain data in a proprietary file format?
- Do you subcontract or outsource any of your data storage?
- Do any independent third parties audit your security practices?
- Have you ever had any data breaches? If so, what did you do?
- What is the longest period your system has been “down”?
- Are the terms of your service agreements negotiable?
- What type of liability coverage do you have?

Typical components of cloud contracts

- Terms of use, including software licenses
- Service Level Agreement (SLA)
- Privacy policy
- Acceptable use policy

Basic terms and conditions

- Price, description of what is being purchased
- School equipment, configuration requirements
- Schedules, term of contract, renewal options
- Termination provisions, status of data upon termination
- Training, documentation
- Data conversion, interface development, if necessary
- Maintenance and support
- Software updates, upgrades

Service Level Agreement

- SLA states predefined service levels and the vendor's payment if those service levels are not achieved.
- SLA should specify each service level, how compliance will be measured, how failures will be reported, and the compensation for each failure.
- Instead of measuring performance by simple uptime, SLAs should specify user metrics such as page rendering time, response time, and user interactivity time.
- SLA should also specify maintenance periods and other periods of unavailability.

Limits on contract enforceability

- Recognize logistical difficulty of litigation against vendor 3000 miles away
- Consider proof problems in a case involving loss or breach of computer data
- Plan for service provider's assertion of operational errors by teachers and students
- Venue and choice of laws provisions are important.

Data security

- Data security is important not only for student records but also district operations.
- Consider the need for third party audit of provider's security procedures.
- There are two standards relevant to certain cloud providers: ISO 27001 (Information Security Management Systems – Requirements) and Standards for Attestation Engagements (SSAE) 16. Ask about vendor compliance.
- Establish notification procedures in case of breach.
- Talk with IT staff and vendor about data backup and recovery.

Mission critical applications

- Some SaaS applications, such as MUNIS, are mission critical because they generate a district's financial records.
- Districts must have access to such data 24/7 for regular operations as well as for reporting, audits, budgeting, etc.
- For such applications, robust contract provisions for data security, redundancy, and recovery are especially important.

Mission critical applications (continued)

- Contracts should ensure that the district can run necessary weekly, monthly, and annual reports and data backups for auditors, reporters, and FOIA requestors.
- Service providers and IT staffs generally think cloud storage is safe. However, attorneys should talk with IT about whether their clients should run hard copies of reports as well as maintain electronic files for data audit trails.

Complying with FOIA requests

- Contracts should ensure that the district will be able to answer valid FOIA requests. This involves two related issues:
    - The contract must explicitly recognize the district's right and obligation to provide responsive records.
    - The contract must ensure an efficient way for the district to search, find, and produce the requested records on a timely basis.

State record retention laws

- State record retention laws mandate both the retention and destruction of public records at specified intervals.
- During contract negotiation, check with IT to determine how the public records created or stored under the contract will be categorized, time-stamped, and retained/destroyed as required.
- Depending on the data, include contract provision recognizing retention and destruction requirements.

Protecting metadata

- Metadata is data about the data, *e.g.*, the name of a file's author, the date the file was created, etc.
- Depending on the contract, cloud providers may collect metadata in cloud data.
- Contract should specify the types of metadata collected, who owns the metadata, what metadata is stored, each party's right to use the metadata, and the client's opt-out for collection and use.

Electronic discovery/spoliation of evidence

- For litigation purposes, electronically stored information includes not only the text of a document and attachments but also metadata and non-rendered file content (data not explicitly displayed).
- Litigation holds of electronically stored information are much more problematic when someone else stores your data. These should be specifically considered during contract negotiation.

Electronic discovery/spoliation of evidence

- Systems of service providers may not preserve metadata or non-rendered file content.
- Contract should be clear about what ESI is stored and how vendor will safeguard ESI when there is a litigation hold.
- Best protection is to have full image/backup of all remotely held ESI as of date of litigation hold (as well as a freeze on deletions on local computers).

Encryption

- One method of data security is encryption of data.
- Data encryption methods vary widely, so it is important to understand and specify in the contract the encryption methods that will be used.
- Include, where possible, contract provisions for encryption of data at rest in school district, in transit to and from the service provider, and at rest in the third party data center.

Foreign data centers

- Financial incentive for foreign data storage countries
- Logistical problems
- Different privacy and data protection laws
- Ask about locations and try to require domestic data storage.

Data upon termination

- Specify use and ownership of data upon contract termination.
- Specify period during which data will be retained after termination.
- Specify format for data storage and format in which data will be returned after termination.
- Specify data destruction at end of retention period after termination.

Compliance with state laws

- In addition to compliance with federal privacy protection statutes such as FERPA, contracts should require service provider compliance with your state's laws.
- For example, 47 states have statutes requiring entities to notify individuals of security breaches of personally identifiable information. *See* http://www.ncsl.org for list
- At least 32 states have data disposal laws that require entities to destroy, dispose, or otherwise make personal information unreadable. *See* http://www.ncsl.org for list

Incorporation by reference

- Documents incorporated by reference, *e.g.* , software license, equipment requirements
- Read incorporated documents
- Modify incorporated documents
- Resolve inconsistencies among documents

Unilateral changes in terms

- Some service provider contracts reserve the right to change terms either without notice or the right to terminate and get a pro-rata refund if the client disagrees after being notified about the change in terms.
- Try to strike such a right which could allow a vendor to change crucial terms about data ownership, data uses, data security, foreign data centers, etc. But deletion will be tough for standard data storage.

2015 COSA School Law Practice Seminar

Negotiating Contracts for Cloud Computing

Additional resources

- Michael E. Casey, *Cloud Computing Contracts* (including links at end of article) http://www.michaelecasey.com/?p=215
- Joe McKendrick, 9 Questions to Ask before Signing a Cloud Computing Contract http://www.forbes.com/sites/joemckendrick/2013/01/14/9-questions-to-ask-before-signing-a cloud-computing-contract/
- Morrison & Foerster LLP, Client Alert, *Negotiating Cloud Contracts*
- Stephanie Overby, *How to Negotiate a Better Cloud Computing Contract* http://www.cio.com.au/article/344007/how_negotiate_better_cloud_computing_contract/
- NIST Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* (December 2011) (intended for federal agencies)

Finding sample contract provisions

- *Protecting the School District in Contracting for Purchases of Hardware and Software*, 2006 NSBA School Law Seminar
- *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service*, Privacy Technical Assistance Center (online)
- GSA Security Language for IT Acquisition Efforts, CIO-IT Security-09-48, Revision 1 (online)