Software IA In The Cloud

Part 2: Records And Databases

*By Dwight Olson**

Having discussed in Part 1, one of a myriad of issues with software applications moving to the cloud, what about the issues of digital data housed in the cloud of electronic databases across the globe? Data may not be protected as IP, but it certainly is a valuable intellectual asset. In the past, data was considered owned by the licensees—at least that's what they would contend. Historically most corporate data was controlled by the software run in protected information technology (IT) departments; governance was done by IT personnel who were employees of the company and charged with the responsibilities of maintaining and securing that data.

"What do senior software executives predict about cloud computing for the next three to five years? One thing is clear: the software industry is in the middle of a major inflection point not seen since the client-server days. The year 2011 is already proving to be a decisive one for cloud software and services vendors. Like a tidal force's change in direction that affects the entire Earth, there are indicators that the world of software is shifting to the cloud. The new market reality is that—no matter their size—software vendors can no longer simply push customers to their products; rather, vendors' products need to be where their customers want to be—in the cloud."[1]

Update. Amazon struggles to restore its Web services business. "As technical problems interrupted off-site data storage provided by Amazon for a second day Friday, industry analysts said the troubles will prompt many companies to reconsider relying on remote computers beyond their control…The problems companies reported ranged from being unable to access data to sites being shut down"[2]

This is a wake-up call for cloud computing and, as Mr. Lohr points out in his article, this will be a start of the re-examination of the contracts (read here LES, licenses) that cover cloud services. So as we begin this reexamination, where are we? Can we get a handle on issues so we can help our companies and clients, be they users or vendors?

Until today, most data resided behind the walls of the company's data center where security, retention and backup were of primary concern. That is, keeping data safe from migration outside the company, keeping the data only as long as required for legal reasons (or if vital digital records, forever), ensuring data consistency (its validity, accuracy, usability and integrity), and keeping the data backed up in case of an IT data center disaster. These were the nightmares of the IT department.

■ Dwight Olson,
V3Data, Principal
San Diego, CA, USA
Chair, LESI IP Valuation Committee
E-mail: dolson@V3Data.com

To complicate these four nightmares, data is becoming a valuable asset and may be generating revenue directly by licensing (via software as a service contract) or indirectly for the company. In the cloud we might find licensors, licensees and other stakeholders fighting for revenue and access without consideration of any rules of the road. Data migrating to the cloud is moving responsibility for its governance out of the hands of the corporation and into the cloud service providers. So as we watch these new information infrastructure cloud providers emerge, where will the governance be, who will responsible, and what safety valves will we find.

Some Background

We have over the past ten (10) years just begun to learn about the Internet's potential use and dangers. We have financed billion dollar corporations such as Semantic to help us fight spam, hackers, and disasters for our pc users connected to the Internet. Who and what will we need to finance as the global information highway connects the cloud infrastructure where applications and data are distributed? Who is in the cloud infrastructure to protect data? For example, our IT departments are just learning to safely use the Internet for backup of corporate pc and server data. Many have concerns about governance over these off-site archives. Even with the data encrypted and sent securely to off-site electronic backup archives. Our IT departments may need to help provide governance

1. *www.SandHill.com* , March 9, 2011 newsletter, "The business strategy destination for enterprise software executives."

2. Saturday April 23, 2011, San Diego Union article, "Outage casts doubts on Cloud Storage" by Steve Lohr.

over the SAAS, IAAS, and PAAS service providers. If they can! Data backup of these new infrastructure cloud servers will be of co-mingled and multiple corporate data. If you're uncomfortable about your corporate data at a cloud service provider, what about that same data backed up to other cloud electronic archives? If any backup exists! For the ultimate user he/she no longer knows where the data is housed or on how many electronic archives holds the data or even how to restore?

On Security and Cryptographic

Fueled by the immense opportunity to use cloud computing by the global community there needs to be a very significant wave of security concerns. In the past, computer security remained a constant race between increased exposure of threats on one hand, and improving policies and technologies to combat them on the other. Over the past 20 years, we've witnessed numerous business re-engineering efforts, these efforts led to higher interest levels in computer security and resulted in additional functions of computer security applications. Examples include: access controls, electronic banking controls, security evaluation certification centers, anti-virus technology and distributed environments. These advances were mostly driven by the IT departments of Corporate America who were responsible for mitigating risk of the data center. But, not the cloud's.

It has been said that we are entering an era of information anywhere, anytime. The problem is that this information arena will probably include much that we do not wish to share with everyone. The full realization of this digital millennium will not come to fruition until we can conduct all of our business and personal communication transactions in a secure, trusted and reliable environment.

Public key cryptography allows for secure authenticated transactions with any party, known or unknown, with assurances of data integrity and non-repudiation of the transaction. Some of these features have been built into current Internet and cloud computing and provide a basis for the secure network needed to support electronic commerce from point to point. That is the information highway now appears to be safe, but are the application and database servers that connect to the information highway safe? Corporations that undertake to provide primary database services on the information highway and provide security and retention of cloud computing need to address the issue of retention and security of housing digital data in the cloud besides its safe secure transport.

A primary method used to address protection of data is encryption. Users and corporations who fear the consequences of losing access to cloud data must begin to understand who is responsible for what is happening in the cloud to "their" secure data. For example, a simple fact from the mid 1990s was that loss of a cryptographic key used for encryption meant loss of the data. An issue we will all watch play out as encryption is used in the cloud to protect privacy and who has access to the decryption keys in the cloud.

What was learned in the 90's might be helpful to mitigate this risk as use of encryption grows. In the past we saw a demand for a trusted third party to participate in the encryption market as one solution to protecting access to globalized encrypted data. See also, "An escrowed encryption system can use cryptography for purposes other than data encryption, for example, user authentication, data integrity, digital signatures, key establishment, and key escrow" from "A Taxonomy for Key Escrow Encryption Systems" by Dorothy E. Denning, Georgetown University and Dennis K. Branstad from Trusted Information Systems.

On Electronic Archives

The huge paper conduits that have been the nerves of commerce are being rapidly replaced by computerized messages and electronic paper. What in the world are we going to do if we do not have paper backup? Where will we find the originals? Using electronic records in replacing paper backup may make the future very different. What will be the new paper backup procedures, how will we authenticate, and will there be paper trails? For example the validity of the computer researches notebooks, or the validity of electronic records for the patent office. Just how do we replace the paper world? We have been working on these issues for years and now we will complicate the issues with globalized digital data and records.

The current practices of using computers and having paper backups for security may have resulted in bearable risks, but what happens when all we have are electronic records? For example in combination, SEC Rules 17a-3 and 17a-4 require broker-dealers to create, and preserve in an easily accessible manner, a comprehensive record of each securities transaction they effect and of their securities business in general. These requirements were integral to the Commission's investor protection function because the preserved records were the primary means of monitoring compliance with applicable securities laws, including antifraud provisions and financial responsibility standards. Recent events involving Wall Street have affirmed the need to have measures in place to protect record integrity.

On USA's SEC Example of Risk Management for Security Records

A close look at the USA's Securities and Exchange (SEC) solution to records integrity and maybe we can learn some for our cloud providers. In a letter from Mr. Michael D. Udoff in 1992, of the Securities Industry Association to the SEC, he noted that until 1970, paper was the sole medium for the preservation of Broker and Dealer (B/D) records, and in 1970 the commission amended the rule to permit microfilm, and in 1979 further amended to permit microfiche. In this letter, he has requested that the SEC Commission take no action if brokers and dealers maintain the required records only on optical disk storage and follow the requirements (outlined in his letter) for replacement of microfilm as backup.

In 1997, the Commission amended paragraph (f) of Rule 17a-4 to allow broker-dealers to store records electronically.[3] The rule, by its terms, does not limit broker-dealers to using a particular type of technology such as optical disk. Instead, it allows them to employ any electronic storage media, subject to certain requirements, including that the media "preserve the records exclusively in a non-rewriteable, non-erasable format." This requirement does not mean that the records must be preserved indefinitely. Like paper and microfilm, electronic records need only be maintained for the relevant retention period specified in the rule. See Exhibit A at the back of this article for salient parts of this ruling. Please note the bold and highlighted sections for requirements beyond just a "backup" copy. These sections deal with duplicate, verifiable, non-destructive, audited, escrowed, and third party access. Wow! So as we move to only digital data, what from the SEC might we learn?

Electronic archiving of records and databases has similar issues to the SEC. For example, one of the primary concerns is that the technology used in the future may not be compatible with current logical records and/or physical media. How many of you have a 5 ¼ inch floppy disk system? Archive (and backup) procedures for records, indexes and computer systems on behalf of a business entity is a complex issue and ideally addresses controlled access to retained materials and the audit of the corresponding software system so that the entity's electronic records are valuable and can be retrieved. In some situations, such as the SEC, the archival guidelines also must provide for an escrow agent's administrative, operational and technical system's integrity or the electronic operational structure to be highly reliable so that a copy of a deposit (or archived document) could be relied upon after retrieval, or in the event of a dispute regarding a document, for authenticity or timeliness.

Another important issue that must also be addressed is the maintenance of the sanctity and readability of the records when those records are dependent on particular and ephemeral technologies and software packages. In the absence of general and widely-accepted standards for the maintenance of long-lived electronic archives, procedures, for example, archiving of hardware and software, secure forward copying, *etc.*, must be defined to ensure that records remain secure and readable for a specified future period and, if necessary, indefinitely. For example, a business entity that uses electronic commerce would be required to archive a variety of records/documents, will generally fall into two categories: journalizing the records and actions relative to the integrity, such as in the security of the system itself, and the records that individual users engaging in their future use or protection.

There are a variety of reasons why some electronic commerce information would be archived. A few of these critical areas include but are not limited to, dispute resolution, conformance with legal requirements, tax audit, SEC compliance, banking records, historical purposes, scientific research, documents having continuing or future legal effect, wills, trusts, life estates, prevention of fraud (clinical and engineering testing, priority of invention and discovery). Many issues are yet to be discussed, but some are: ability to retrieve at some distant point in time, usefulness, access control, distributed archival, indexing, compatibility of equipment/formats, standards, archival authority, quality or level of service.

On a Global Example of Risk Management

The Internet Corporation for Assigned Names and Numbers (ICANN) must have been thinking of protecting access to global "cloud" databases and what was needed to help minimize loss of its records—that is access to all Domain Names worldwide. The current version of the ICANN Registrar Accreditation Agreement ("RAA") obliges registrars to periodically submit a copy of their registration database to ICANN or a mutually-approved third-party escrow agent. This escrowed data could be used by another registrar assigned by ICANN (or even temporarily by ICANN itself) to continue the provision of registrar services to the customers of a registrar whose accreditation is terminated or expires without renewal.

3. *http://www.sec.gov/rules/interp/34-47806.htm#P32_4611.*

The Data Escrow provision is set forth in RAA subsection 3.6, provides as follows:

> *"During the Term of this Agreement, on a schedule, under the terms, and in the format specified by ICANN, Registrar shall submit an electronic copy of the database described in Subsection 3.4.1 to ICANN or, at Registrar's election and at its expense, to a reputable escrow agent mutually approved by Registrar and ICANN, such approval also not to be unreasonably withheld by either party. The data shall be held under an agreement among Registrar, ICANN, and the escrow agent (if any) providing that (1) the data shall be received and held in escrow, with no use other than verification that the deposited data is complete, consistent, and in proper format, until released to ICANN; (2) the data shall be released from escrow upon expiration without renewal or termination of this Agreement; and (3) ICANN's rights under the escrow agreement shall be assigned with any assignment of this Agreement. The escrow shall provide that in the event the escrow is released under this Subsection, ICANN (or its assignee) shall have a non-exclusive, irrevocable, royalty-free license to exercise (only for transitional purposes) or have exercised all rights necessary to provide Registrar Services."*

Should We Be Concerned About Ownership, Future Access and Privacy of Our Data? YES!

Here is an excerpt from an email sent from AOL dated 2/20/2011 to its users on updated "Terms of Service and Privacy Policy for AOL Users." Who is the owner? Most interesting email and service license!

> *Dear AOL Users,*
>
> *AOL is working hard to change and improve the way we serve you across all aspects of our services. We have recently relaunched and improved many of our consumer experiences, including AOL.com and MapQuest.com. As we continue to improve AOL for you, some of the improvements are updating the ways that we interact with you and your information. As a result, we want to update you on our Terms of Service (TOS), which contains the agreements between you and AOL.*
>
> *In addition, we are also updating our Privacy Policy. Privacy is incredibly important to all of us and we want to present the updates to our privacy policy in a simplified format designed to help clarify what information we collect, how we use it, and the marketing preferences and online advertising choices available to you. Both the updated TOS and Privacy Policy are available online now and will take effect on March 31, 2011.*
>
> ***[Below is what was buried in the policy list]:***
>
> ***We clarify that for content you post on any AOL sites, you continue to own the content and AOL has the right to use and share your content.***

AOL is not alone, read what Google's license says. You give a license to them for all content and permission to republish.

Section *"11.1 You retain copyright and any other rights you already hold in Content which you submit, share, upload, post or display on or through, the Service. By submitting, sharing, uploading, posting or displaying the Content you give Google a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, share, upload, post or display on or through the Service for the sole purpose of enabling Google to provide you with the Service in accordance with the Google Docs Privacy Policy."*[4]

For Those Who Think Your Records Are Retained For You—NOT

Archiving in the cloud has been rapidly growing in popularity, offering a number of benefits, which are attractive to companies of all sizes and all industries. These benefits are especially important in these times of tighter budgets, shrinking IT teams, and increased email volume. However, security and legal compliance of cloud solutions continues to be an area of concern. Then again, who owns and who is responsible and for what? How about what the providers say about retention? Where are health care records going?

Healthcare information technology is entering a new age where Health Information Exchanges (HIEs) and the new Nationwide Health Information Network (NHIN) will provide access to Electronic Health Records (EHRs) stored at every healthcare provider, hospital, clinic and lab. At the same time, the information needs of consumers have been largely ignored. Consumers want access and control of their healthcare records. Today, Personal Health Record systems (PHRs) like Microsoft's HealthVault enable people to track some information on their own, but there is almost no access to the records stored by providers. The government is spending an unprecedented amount (over $25B just in ARRA/HITECH funds) in the current budget to make ubiquitous EHRs and HIEs a reality. However, HIEs will need to generate

4. *http://www.google.com/google-d-s/addlterms.html.*

sufficient revenue to sustain their operations. This must be a key concern of almost every HIE today.

But Then We are Safe with Corporate America—Maybe Not

Most cloud service agreements (that you click through) have a WE MAKE NO WARRANTY statement. As Microsoft summed up in its online service statement:

> *We provide the Service "as-is," "with all faults" and "as available." We do not guarantee the accuracy or timeliness of information available from the Service. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws that this Service Agreement cannot change. We exclude any implied warranties including those of merchantability, fitness for a particular purpose, workmanlike effort and non-infringement.*
>
> *Programs and devices that connect with HealthVault are not endorsed or warranted by Microsoft. Product descriptions are by their manufacturers and provided for informational purposes only. We do not operate, control or supply any information, product, or service that is not clearly identified as supplied by Microsoft. This site does not provide medical or any other health care advice, diagnosis or treatment. Always seek the advice of your physician or other qualified health provider with any questions you may have regarding a medical condition, diet, fitness or wellness program. Never disregard professional medical advice or delay in seeking it because of information you accessed on or through the Service.*
>
> *You can recover from Microsoft only direct damages up to an amount you pay Microsoft for this Service. You cannot recover any other damages, including consequential, lost profits, special, indirect, incidental or punitive damages.*
>
> *This limitation applies to anything related to:*
>
> *• The Service,*
>
> *• Content (including code) on third party Internet sites, third party programs or third party conduct,*
>
> *• Viruses or other disabling features that affect your access to or use of the Service,*
>
> *• Incompatibility between the Service and other Services, software and hardware,*
>
> *• Delays or failures you may have in initiating, conducting or completing any transmissions or transactions in connection with the Service in an accurate or timely manner, and*
>
> *• Claims for breach of Service Agreement, breach of warranty, guarantee or condition, strict liability, negligence, or other tort.*
>
> *It also applies even if:*
>
> *• This remedy does not fully compensate you for any losses, or fails of its essential purpose; or*
>
> *• Microsoft knew or should have known about the possibility of the damages.*
>
> *Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.*
>
> *Changes to the Service; If We Cancel the Service.*
>
> *We may change the Service or delete features at any time and for any reason. We may cancel or suspend your Service at any time. Our cancellation or suspension may be without cause and/or without notice. Upon Service cancellation, your right to use the Service stops right away.*

When cloud storage providers shut down, as four have done in the past year of 2010, users are left wondering how they'll get their data back and whether they'll be able to migrate it directly to a new service provider. More importantly, analysts say, what guarantees do they have that the data stored offsite will be deleted after the shutdown. Currently, there is no direct way to migrate data to another provider, and there are no government rules or regulations specific to data managed by cloud storage providers.[5]

Over the past year, four cloud storage service providers have said they're shutting down and Amazon's cloud services have been problematic. "All of these things are coming together... to give cloud storage providers a black eye. Anyone who was on the fence about cloud storage may be off of it by now," said Gartner research analyst Adam Couture. More importantly, the closures and outages leave users with an important question: What happens to their data when the cloud they use evaporates? Currently, there's no way for a cloud storage service provider to directly migrate customer data to another provider. If a service goes down, the hosting company must return the data to its customer, who then must find another provider or revert back to storing it locally, according to Arun Taneja, principal analyst at The Taneja Group.[6]

---

5. *See http://hardware.slashdot.org/stry/11/04/26/1425255/What-Happens-To-Data-When-a-Cloud-Provider-Dies?utm_source=headlines&utm_medium=email.*

6. *See http://www.computerworld.com/s/article/9216159/What_happens_to_data_when_your_cloud_provider_evaporates_.*

We have issues here in North America, perhaps globally, not only about the ownership and rights to data (generally conceded to be the property of the holder) but even the laws in Canada and the U.S. are not clear on that point even the right to mine or not mine that data. To be able to aggregate data yet to protect the secrecy of each original owner has great value. Mined and aggregated data has value, the key is to know how to protect and license appropriately. If we permit mining via license can we in the reverse license or contract that data will not be mined? In the energy service sector, the customer does not have enough data to be statistically valuable or possibly valid. Validity and value may only come when combined with other customer's data. Aggregation has value in the context of clinical health and also in oil and gas production to name just a few. Cloud computing "lets" the service provider mine data, but how do we deal with ownership, recovery, control and value propositions. Cloud computing only makes these issues more complex with loss of direct physical access over the data. We need to think clearly about the issues and perhaps include new terms in our "cloud licenses" just as ICANN did. Maybe we should think about data as "trade secrets" or provide provisions for third party audit (similar to a financial auditor) that monitors integrity. These would be a good start for LES licensing professionals.

Welcome to the cloud! ■

**Submitted on behalf of the LESI IT Ecommerce Committee.*

Exhibit A (From SEC 17 a-4) Preservation of Digital Records

(ii) The electronic storage media must:

(A) Preserve the records exclusively in a **non-rewriteable, non-erasable format**;

(B) **Verify automatically the quality and accuracy of the storage media recording process;**

(C) Serialize the original and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media; and

(D) Have the capacity to readily download indexes and records preserved on the electronic storage media to any medium acceptable under this paragraph as required by the Commission or the self-regulatory organizations of which the member, broker, or dealer is a member.

(3) If a member, broker, or dealer uses micrographic media or electronic storage media, it shall:

(i) At all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.

(ii) Be ready at all times to provide, and immediately provide, any facsimile enlargement which the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer may request.

(iii) **Store separately from the original, a duplicate copy of the record** stored on any medium acceptable under Sec. 240.17a-4 for the time required.

(iv) Organize and index accurately all information maintained on both original and any duplicate storage media.

(A) At all times, a member, broker, or dealer must be able to have such indexes available for examination by the staffs of the Commission and the self- regulatory organizations of which the broker or dealer is a member.

(B) Each index must be duplicated and the duplicate copies must be stored separately from the original copy of each index.

(C) Original and duplicate indexes must be preserved for the time required for the indexed records.

(v) The member, broker, or dealer must have **in place an audit system** providing for accountability regarding inputting of records required to be maintained and preserved pursuant to Sec. Sec. 240.17a-3 and 240.17a-4 to electronic storage media and inputting of any changes made to every original and duplicate record maintained and preserved thereby.

(A) At all times, a member, broker, or dealer must be able to have the results of such audit system available for examination by the staffs of the Commission and the self-regulatory organizations of which the broker or dealer is a member.

(B) The audit results must be preserved for the time required for the audited records.

(vi) The member, broker, or dealer must maintain, keep current, and provide promptly upon request by the staffs of the Commission or the self-regulatory organizations of which the member, broker, or

broker-dealer is a member all information necessary to access records and indexes stored on the electronic storage media; or **place in escrow and keep current a copy of the physical and logical file format of the electronic storage media**, the field format of all different information types written on the electronic storage media and the source code, together with the appropriate documentation and information necessary to access records and indexes.

(vii) For every member, broker, or dealer exclusively using electronic storage media for some or all of its record preservation under this section, **at least one third party ("the undersigned"), who has access to and the ability to download information from the member's, broker's, or dealer's electronic storage media to any acceptable medium under this section**, shall file with the designated examining authority for the member, broker, or dealer the following undertakings with respect to such records:

The undersigned hereby undertakes to furnish promptly to the U.S. Securities and Exchange Commission ("Commission"), its designees or representatives, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer, upon reasonable request, such information as is deemed necessary by the staffs of the Commission, any self-regulatory organization of which it is a member, or any State securities regulator having jurisdiction over the member, broker or dealer to download information kept on the broker's or dealer's electronic storage media to any medium acceptable under Rule 17a-4.

Furthermore, the undersigned hereby undertakes to take reasonable steps to provide access to information contained on the broker's or dealer's electronic storage media, including, as appropriate, arrangements for the downloading of any record required to be maintained and preserved by the broker or dealer pursuant to Rules 17a-3 and 17a-4.