



Cloudy Privacy Computing

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI
Final Draft for December 2008 CSI Alert

Is cloud computing cumulous or cirrus?

At Thanksgiving dinner, some of my relatives (none of whom are in the IT, information security or privacy industries) asked what I was writing about now. I mentioned that I was looking into the privacy implications of cloud computing. After some silence and a few shared glances at each other, one asked, “Are cumulous more dangerous than cirrus to computers?” The concept of “cloud computing” is not well known by most folks. Certainly not the personnel using a vast and growing number of cloud computing applications, without even know it, from business networks. If they don’t know what they are using, then how can they know the information security and privacy risks involved?

“Cloud computing” floated across the IT horizon in 2008 to become one of the hot topics of conversation for most IT leaders. For those who may wonder, cloud computing is a nebulous (or should I say cumulous) term used to describe any of a number of services or applications that many businesses, as well as individuals, use that are actually located outside the network perimeter and on other entities’ servers accessible via the Internet. They are very much like silent business partners.

What’s to worry about?

Are those silent business partners securing their servers appropriately, and ensuring appropriate privacy protections to the vast amounts of personally identifiable information (PII) that is being entrusted to them? Is there any need to worry? And what about how storing data on, and communicating via, clouds impacts compliance?

While at the recent CSI Annual conference in National Harbor, Maryland, I asked a few executives in attendance what they worried about with regard to security and privacy issues related to cloud computing. One, a very smart security vendor VP, said there were no new issues, just issues that needed to be revisited. So, he had no worries. Is it really that simple? Another, a brilliant IT services vendor VP, said that the more she learned, the more concerned she became, and that she was sure she still hadn’t heard the worst.

Here are a few of the worries I have with cloud computing as they relate to privacy and information security:

- Who has access to the information organizations are putting on these external cloud application and systems servers?
- How does an organization’s compliance posture for applicable laws, regulations, standards, contracts and policies change when business, and sometimes even customer and employee, information is stored in the clouds?
- How long does information put into the clouds stay in those clouds? Do the clouds have retention policies? Can information be permanently and completely removed from the clouds once it is put there?



- Are there any logs generated to show how that cloudy information is accessed, copied, modified and otherwise used?
- Can all necessary information in clouds be easily retrieved during e-discovery activities? If so, what are the related costs involved?

Consider a couple of popular cloud computing services, Google Documents (Google Docs for short) and Adobe Photoshop Express.

No worries at Google Docs?

This summer I participated in a group project of globally spread information security and privacy experts, and we used Google Docs as the primary repository for our work, none of which was classified as sensitive or confidential. I sometimes pondered similar questions related to the documents we put in the Google Docs cloud.

The Google Docs site indicates they use the same privacy policy as the one located at the primary Google site in addition to some other stipulations. Basically there is very little expectation of tight controls to the files put onto the site; security is pretty much left up to the site users. And that amount of security is pretty limited, considering Google Docs indicates that the files you entrust to them may be “read, copied, used and redistributed by people you know or, again if you choose, by people you do not know. Information you disclose using the chat function of Google Docs may be read, copied, used and redistributed by people participating in the chat.” Google Docs gives a nonchalant warning to “Use care when including sensitive personal information in documents you share or in chat sessions, such as social security numbers, financial account information, home addresses or phone numbers.”

It was good to see Google Docs indicates that you may “permanently delete” files from their systems, but then in the next sentence states that “Because of the way we maintain this service, residual copies of your files and other information associated with your account may remain on our servers for three weeks.”

It appears that Google Docs could be a great way to collaborate with other organizations on documents that are not sensitive in nature, but probably not a repository to place PII or business sensitive information within.

No worries with Adobe?

Many of the folks I know, including one of the parents’ groups I belong to, use Adobe Photoshop Express to share photos; hey, it’s quick and easy! I know some businesses that are also using this site to share files with business partners. Does Adobe protect those photos and answer my questions from earlier? It is important to also consider that some of those photos could be interpreted incorrectly taken out of context if viewed by unauthorized or unintended individuals.

The privacy policy from the Photoshop Express site is the same one as used from the Adobe home page. It is quite wordy, lengthy, is heavy in legalese, and includes several implied consents. For example, it states that, “However, if Adobe sells assets (or the assets of a division or subsidiary) to another entity, or Adobe (or a division or subsidiary) is acquired by or merged with another entity, you agree that Adobe may



provide to such entity customer information that is related to that part of our business that was sold to or merged with the other entity without obtaining your further consent.”

Another implied consent states, “By using this Site and the Products and Services, you agree and acknowledge that personal information collected through the Site or in connection with the Products and Services may be transferred across national boundaries and stored and processed in any of the countries around the world in which Adobe maintains offices, including the United States. You also acknowledge that in certain countries or with respect to certain activities, the collection, transfer, storage, and processing of your information may be undertaken by trusted third party vendors or agents of Adobe such as credit card processors, shipping agents, web hosting providers, mail and email service providers and web analytic providers, to help facilitate Adobe in providing certain functions.”

And the following is an example of some of the muddled statements within the policy, “Adobe does not share personal information it receives from residents of California or from residents of any other place with such Providers for the Providers’ own marketing purposes unless Adobe has received an opt-in from you.” Huh? Aren’t all folks who are not a resident of California then residents of some other place?

It is not clear how long Adobe retains information put on their servers, or how you can completely remove information from the site. Here is one statement regarding retention, “If you are invited by someone else to participate in shared editing or viewing of documents, photos, websites or other content, you will typically be required to contact the person who invited you to update, correct or delete the personal information they provided about you. In general, even though we may delete an account you hold with us in these types of shared editing or viewing areas, we may continue to retain information regarding your past actions with respect to content reviews or sharing initiated by others.”

I could find nothing related to removal or retention of the photos on the site. It looks like a great way to share non-sensitive photos, but it would not be wise to use it for business purposes without first doing a thorough information security and privacy program and review of the site.

Cloudy laws and regulations issues

In the past many organizations found themselves in complicated and sticky situations by addressing compliance issues only after new technologies and tools were widely used throughout the enterprise. Addressing all those issues after the fact is always exponentially harder than addressing them before new applications, systems and tools are already imbedded within the organization and already considered as being indispensable. In some organizations it is likely that this is already be the case with cloud computing. If so, address the issues now before use progresses even more deeply within the business architecture. If your organization is not yet using cloud computing, act now to prevent compliance issues from getting out of hand, and to save yourself some headaches.

Before the business commits to cloud computing services, it is good to consider the cloud computing vendor as much more than just a software provider; it really is another



type of business partner. Businesses need to scrutinize the information security and privacy programs and practices of vendors and other business partners, and the cloud computing tools, applications and services should be viewed no differently. If your business is entrusting critical processing and data to another entity, you should first ensure it is trustworthy, secure and will meet your organization's compliance obligations.

Consider all the many different compliance issues. Most laws and regulations, not only in the U.S., but also in many other countries, require organizations to establish appropriate controls and safeguards around PII and related business information. But how do you know that appropriate controls and safeguards exist within the clouds? Information processed in clouds is not under your organization's control. Do you know what happens to the information, where it is stored, who has access to it, and where it goes after your contract with the cloud computing contract ends? All these questions must be answered for a wide range of laws such as HIPAA, GLBA, Canada's PIPEDA, and the EU data protection laws under the EU Data Protection Directive, just to name a few. Consider this; what breach notice actions will you need to take if your cloud computing service has a security incident involving your organization's PII? Will the cloud computing service that had an incident even notify you? And in organizations that process credit card payments there are also certainly compliance issues for PCI DSS compliance to consider when using cloud services that involve customer PII.

Privacy issues still foggy

As companies start using more cloud computing resources for business purposes, business leaders will be wise to identify the sites and services they want to use, or may already be using, and then review the information security and privacy policies and update them accordingly to address these new risks. In addition to usage policies for employee interaction on public sites, companies must look for new ways to protect data on resources that are not under their direct control. This includes securing data as it is transmitted to and stored in the cloud as well as granting the appropriate access rights regarding who can view the data. Select cloud computing services carefully, and with your organization's legal requirements and your own information security and privacy policies in mind.


Here are issues to address and questions to ask when considering a cloud computing service:

- Where will your organization's data be stored?
- Will your organization's data be stored in a way that intermingles it with the data from other companies?
- Who will have access to your organization's data?
- Are backup and recovery processes in place? Are they adequate for your organization's needs?
- What are the availability promises for the cloud service? Are they documented within a Service Level Agreement?
- What audit trails are generated and maintained for your data?
- How quickly will you be able to obtain information about data access and associated logs?



- What laws, regulations, industry standards, contractual obligations, and organizational policies cover the data you are considering to be sent to the cloud?
- Does the cloud computing service have established and documented information security policies and supporting procedures?
- What does the cloud computing service's posted privacy and security policies say? Do they support their internal policies and contractual promises?

Basically you need to ask all the same questions that you would during a third-party, vendor or business partner security program review, in addition to knowing some specifics mentioned above that are unique to cloud computing services.

 BITS provides a fully useable "Standardized Information Gathering" vendor security assessment questionnaire at <http://www.sharedassessments.org/>. I also have a vendor security review tool available at my site, <http://www.privacyguidance.com>.

You also need to ensure your policies and procedures are up-to-date with your new cloud computing activities. Some of the issues to address within your policies and supporting procedures include:

1. The increased risks of inadvertent or deliberate disclosure of sensitive data and PII by posting to cloud computing sites.
2. The increased exposure to malware that is commonly hiding on and distributed through these sites.
3. The increased risk of unauthorized use of the data used on the cloud computing sites as a result of minimal to no access controls.
4. Determining how data protection requirements apply to information stored in these computer clouds.
5. Determining the retention requirements for information put into the clouds. Can information be permanently and completely removed from the clouds once it is put there?
6. Determining the logs that need to be generated and maintained for access to data in the clouds. Determine logs that are necessary to show how information is accessed, copied, modified and otherwise used.

I also recommend organizations do a privacy impact assessment (PIA) whenever considering a move to a cloud computing service, or any type of software-as-a-service (SaaS) solution. As part of the PIA map your PII data flows to identify the vulnerabilities and threats to determine security and non-compliance risks.

Business leaders will be challenged to balance the benefits of cloud computing with the actions necessary to protect business information assets. Committing to a cloud computing service without first considering the legal and compliance risks, and without knowing the security controls that exist, could result in very significant negative business impact from noncompliance and/or security incidents, well beyond the savings that using the cloud service brings to the business. It is worth spending some time to determine how cloud computing may already be used within your organization, the data involved, and the related risks.



Importantly, be sure you provide training and ongoing awareness communications to your personnel about how they can, and cannot, use specific cloud computing services, and make sure they know and follow the associated procedures.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, “The Privacy Professor”™ is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She creates learning tools, such as “Protecting Information” and “The Privacy Professor’s Security Search #1,” and blogs daily at <http://www.realtime-itcompliance.com>. She can be reached at rebeccaherold@rebeccaherold.com or <http://www.privacyguidance.com>.