


 Posted By [Shai Samet](#) | May 09, 2010

## Three steps toward achieving privacy in the cloud

"Cloud computing" may be old wine in a new bottle. But without a privacy gameplan, your company may incur substantial new risk when it moves data to the cloud.

Hiring third parties to store and process data isn't new. Third-party hosted web applications such as Microsoft Exchange have been around since the 1990s. Plenty of confidential employee and consumer information has passed through hosted Exchange servers.

So what is it about cloud computing – or more specifically, outsourcing data to third-party cloud providers – that has so many IT and privacy executives still worried? And what can companies do to address these concerns?

I think there are two things at play: (1) the very insecure-sounding word "cloud" and (2) the idea that data could be anywhere from day to day.

On the first point, network engineers and marketers haven't done us any favors by calling this new method of data management "cloud computing." A cloud is something amorphous with very soft boundaries. It's probably the least-secure thing in creation. Why would any self-respecting company put their most sensitive assets in a cloud? So, on one level, misperceptions are driving concerns.

On the other hand, perhaps the reason the term "cloud" has become so popular is because it somewhat describes the reality – that there may be a large number of servers spread around the world handling a moving set of data.

Let me explain with a personal story. As the owner of a small business, I recently embarked on an online marketing campaign promoting the development and launch of a new product. To get the word out at a minimal cost, I chose to use the cloud services of several different SaaS providers rather than having an engineer build me a customized home-grown solution. I engaged the services of WuFoo (for website forms), PayPal (for payment processing), Constant Contact (for email marketing), and Survey Monkey (for customer feedback and surveys), and that's not even a complete list. In each case, I discovered that the online tool was storing a record of each customer that interacted with that tool, but because the various tools were not fully integrated with one another, I ended up having information regarding the same customers stored in various locations in the cloud. This created a challenge in terms of managing the different storage points, both from a business and compliance standpoint.

For medium-to-large sized enterprises, this issue is magnified tenfold. Various business units within an organization may be utilizing different cloud providers for different tasks, and when done in large quantities across a global company, the result could be a cobweb of data housed in various locations in the cloud and thus on various data servers scattered around the world. For companies based in Europe where the export of personal data to non-European countries is generally forbidden (absent an appropriate cross-border legal mechanism), it pays to be extra alarmed and keep a close tab on where your data is at all times.

The good news is that these risks do not present significantly new challenges. Rather, they demand that we rethink and reapply fundamentally-basic privacy principles that sit at the core of any sound privacy compliance program. These principles include:

- **Vendor Due Diligence ("Doing Your Homework")**

This involves conducting a thorough review of the cloud provider's overall privacy and data security posture, prior to engaging the service. Depending on your company's size and bargaining power (relative to the cloud provider), this may entail the use of written contractual clauses that bind your providers (as well as their subcontractors) to adhere to strict legal frameworks and standards of data security and confidentiality. New U.S. data security and breach notification laws at both the state and federal levels (e.g., HITECH Act, Massachusetts 201 CMR 17.00, etc.), as well as older EU data protection laws, amplify the importance of getting these assurances.

- **Data Inventorying and Mapping ("Knowing Where Your Data Is")**

This refers to the process of taking stock of the various cloud providers engaged by your company, the specific data elements entrusted with each, and (most important of all) the physical locations and servers where the data actually resides or can be accessed and viewed by authorized personnel. This

### Popular Searches

cloud a ca cisco shai lala  
 45% privacy commons apple  
 cloud.com vmware ticketmaster  
 practices president security novell  
 home Storage

exercise must also consider the storage of cloud data on backup servers and the further transfer of cloud data to third party subcontractors. Data inventories and mappings should be documented and updated on a yearly basis.

Sponsored by 

### Ongoing Monitoring and Oversight ("Keeping a Watchful Eye")

These are follow-up measures taken to ensure that your cloud providers continue to meet privacy and data security expectations. Depending on the complexity of your business and pertinent regulations, measures can range anywhere from conducting full-fledged onsite privacy audits to performing random offsite testing. It may be worthwhile to also request a copy of any standardized audit that the cloud provider undergoes as part of an industry standard or data security protocol (e.g., SAS 70, PCI certification, etc.).

It is my belief that IT and privacy execs who put these practices into place ahead of time will be able to sleep better at night, even as their data drifts away in the clouds.

*Posted by Shai Samet, with contributions from Jay Cline*

*Shai Samet is founder and president of Samet Privacy, a boutique consulting practice that specializes in advising and assisting companies with their compliance obligations for information privacy and security. Samet is a consultant, Certified Information Privacy Professional (CIPP), and former attorney with over ten years of exclusive experience in developing and implementing compliant privacy programs and procedures for large consumer-facing organizations, including many Fortune 500 companies. Samet has been recognized by [Computerworld.com](http://Computerworld.com) as a "Best Privacy Adviser" two consecutive years (2007 and 2008) and his firm is listed among "Eight Privacy Firms to Watch." Samet can be reached online at [www.sametprivacy.com/contact](http://www.sametprivacy.com/contact), via email at [shai@sametprivacy.com](mailto:shai@sametprivacy.com), or by phone at (323) 939-3282.*

*Jay Cline is president of Minnesota Privacy Consultants and is the privacy columnist for Computerworld.*

★★★★★ | Comments 2

[Share](#)

5/11/10 6:53 AM by [member CC](#)



Great info here!

[Sign in to vote.](#) [Top](#)

5/17/10 12:54 PM by [Yves LE ROUX](#)



I want to give you an European point of view on this privacy issue in the cloud. In order to do so I will use an excerpt from the European Network and Information Security Agency (ENISA) Report entitled: Cloud Computing: Benefits, risks and recommendations for information security"

"To apply the EU Data Protection Directive adequately, the availability and integrity of data are key, leading the discussion to data security measures. There are unavoidable trade-offs here. More data security is likely to lead to reduced availability. The customer of the cloud provider may thus want to take a close look at the security measures the cloud provider has in place and the data availability guaranteed. It has to be born in mind that in most European countries there are mandatory data security requirements. The customer of the cloud provider will have to make sure those measures are complied with. In some cases (eHealth and, possibly, Resilience scenarios, when sensitive data and financial data are processed) the customer may even want to ensure even stricter data security measures as to the storage of data, communication or transfer of data, data disaster recovery and onward transfer.

It has to be clear at this point that the customer – when classified as sole data Controller - will be the entity responsible for the processing of personal data in relation to the data subjects. The customer will also be responsible for this data when such processing is carried out by the Cloud Provider in the role of external Processor. Failure to comply with the Data Protection Directive may lead to administrative, civil and also criminal sanctions, which vary from country to country, for the data controller. Such sanctions are mainly detailed in the relevant statutory instruments by which Directive 95/46/EC has been implemented in the various EU member States."

[Sign in to vote.](#) [Top](#)

[Privacy Policy](#) | [Terms of Use](#) | [Contact Us](#)  
Copyright © 2010 CA. All Rights Reserved