Data Privacy in the Cloud: A Dozen Myths & Facts
March 7-9 Washington DC

Presented by:
Barbara Cosgrove, Chief Security Officer, Workday, Inc.
Lothar Determann, Partner, Baker & McKenzie LLP
We’re taking on the most common concerns raised against cloud computing solutions as two leading privacy experts provide practical guidance and dispel myths about privacy in the cloud. Hear seasoned experts test the notion that cloud computing presents fundamentally unique data privacy challenges, argue that increased data sharing in the cloud can actually be good for privacy and assert that legal compliance does not fall under service provider purview. These and other major questions are tackled in this session, where you’ll get the information you need to confidently maneuver your organization through the cloud.
What you’ll take away:

- A solid understanding of pros and cons of cloud computing for privacy compliance
- An increased ability to discuss challenges with customers and providers
- Practical guidance for contracts between vendors and customers
A DOZEN MYTHS

Myth 1: Cloud Computing Presents Fundamentally New and Unique Challenges for Data Privacy and Security Compliance

Myth 2: Cloud Computing Involves More Data Sharing, Which Is Inherently Bad for Privacy

Myth 3: Cloud Computing Is Bad for Data Security

Myth 4: Cloud Computing Causes Additional Issues Under Privacy Law Because Data Is Transmitted Internationally

Myth 5: Data in the United States Is Endangered by the USA Patriot Act

Myth 6: Record Keeping Laws Require Data to Stay Local

Myth 7: US-EU Safe Harbor Does Not Apply to Service Provider Arrangements

Myth 8: Contractual Clauses Are Unnecessary If the Service Provider Is Safe Harbor-Certified

Myth 9: Data Privacy & Security Law Compliance Is the Provider’s Responsibility

Myth 10: Cloud Service Providers Cannot Cede Control to Their Customers

Myth 11: Vendor Has and Should Accept Unlimited Liability for Data Security Breaches

Myth 12: Customer Must Have the Right to Access the Provider’s Data Centers and Systems for Audit Purposes
Myth 1: Cloud Computing Presents Fundamentally New and Unique Challenges for Data Privacy and Security Compliance
Fact is that consumers and companies have been entrusting specialized service providers with personal data for a long time:
- including telecommunications companies, payment processors, accountants, and various outsourcing service providers (e.g., payroll, call centers, and IT support)
- Internet is founded on the principle of decentralized transfer of data across geographies, devices, and connections.
– Remember “application service providers”? 

Myth 1: Cloud Computing Presents Fundamentally New and Unique Challenges for Data Privacy and Security Compliance
Myth 2: Cloud Computing Involves More Data Sharing, Which Is Inherently Bad for Privacy
Myth 2: Cloud Computing Involves More Data Sharing, Which Is Inherently Bad for Privacy

Fact is …

… sharing with processors ≠ transfers to controllers.

… companies never act without people, and people can be statutory employees, individual independent contractors or employees or contractors of corporate suppliers – neither option is per se harmful to data privacy.

… data sharing with data processing agents is not inherently bad or good for privacy; it is neutral…

… most multinational companies transfer data across geographies anyhow.
Myth 3: Cloud Computing Is Bad for Data Security
Fact is …

… whether personal data is safer on a system secured by you or your vendor depends on who you and your vendor are, depends on the security measures deployed by each particular organization.
For example regarding a global HRIS, each multinational employer needs to ask itself whether its own IT capabilities and security policies are superior to the measures deployed by a specialized vendor that can leverage economies of scale and is motivated by the risk of reputational harm to keep data of its customers secure.
Myth 4: Cloud Computing Causes Additional Issues Under Privacy Law Because Data Is Transmitted Internationally
Myth 4: Cloud Computing Causes Additional Issues Under Privacy Law Because Data Is Transmitted Internationally

Fact is that most companies are already transmitting data internationally because they use the Internet (for example, to email spreadsheets to various office locations) or because they have subsidiaries, customers, suppliers, or channel partners in other jurisdictions.
Myth 5: Data in the United States Is Endangered by the USA Patriot Act
The United States enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) in October 2001 following the September 11 terrorist attacks to help fight terrorism and money laundering activities and to provide certain additional investigative powers to US law enforcement officials.
But:

- these powers are not relevant for most types of data in cloud computing arrangements;
- the government is much more likely to obtain the data directly from the data controllers (i.e., users of cloud computing services);
- if the data controller is not based in the United States and lacks a strong nexus to the United States, chances are the US government is not interested in the data regardless of whether the data is hosted in the United States;
- if the US government is interested, it can usually obtain access to the data through foreign governments through judicial assistance and cooperation treaties, regardless of where the data is hosted;
- similar powers exist in most other countries and data is typically much more at risk of being accessed by governments at the place where the data controller is based; and
- the USA Patriot Act issue is cited to support unrelated agendas, such as protecting local companies or unionized jobs from global competition.
Myth 5: Data in the United States Is Endangered by the USA Patriot Act Contd.

The information that the US government seeks to fight terrorism and money-laundering is not what most companies store or process in the cloud...In some cases, the additional hurdles established by jurisdictional complications will make a difference, but this difference works both ways. For example, a US bankruptcy court recently refused to hand over emails to and from a German resident to the German government...
In this case, the German resident’s privacy was better protected due to the fact that his emails were stored in the United States: The German government would have easily gotten access to his email if he had used a German Internet service provider.

Most countries around the world allow law enforcement access to private information to a similar extent as in the United States, and many countries have updated their privacy laws to provide for minimum data retention requirements (European telecommunications laws go beyond US requirements) and otherwise lowered privacy protection standards.
Myth 6: Record Keeping Laws Require Data to Stay Local
Myth 6: Record Keeping Laws Require Data to Stay Local

Fact is that some tax, bookkeeping, and corporate laws in some jurisdictions historically required certain records to stay in country.

But such requirements apply only to certain kinds of records and they do not prohibit the transfer of data into the cloud so long as originals or back-up copies are also kept local.
Myth 7: US-EU Safe Harbor Does Not Apply to Service Provider Arrangements
Fact is that the safe harbor principles expressly state that data processors may participate and achieve adequacy through certification and that the EU Commission ordered EEA member states to consider companies “adequate” if they certify under the US-EU safe harbor program whether they act as data controllers or processors.

Consider – is data really safer in every EEA Member State than anywhere in the USA?
Myth 8: Contractual Clauses Are Unnecessary If the Service Provider Is Safe Harbor-Certified
Fact is that the safe harbor certification qualifies a service provider outside the EEA as “adequate” as a service provider within the EEA is presumed to be.

But, European laws require particular contractual clauses for data transfers to any service provider, whether the provider is in the EEA or outside…

You have to clear three hurdles…
Myth 9: Data Privacy & Security Law Compliance Is the Provider’s Responsibility
Fact is that data privacy and security laws primarily hold the data controller responsible for compliance, that is, the customer in a service provider relationship.

The service provider has typically only two duties under data privacy laws: The processor has to follow its customer’s instructions and keep the data secure against unauthorized access.

It is important for customer and vendor to reach a reasonable agreement about what level of security is appropriate for particular types of data and who should be doing what...
Myth 10: Cloud Service Providers Cannot Cede Control to Their Customers
Fact is that many organizations find it difficult to stay in control over modern IT systems, whether they hire service providers to provide IT infrastructure or whether they host, operate, and maintain systems themselves.
Myth 11: Vendor Has and Should Accept Unlimited Liability for Data Security Breaches
Fact is that service providers may not always be able to limit their liability vis-à-vis the data subjects.

But, data protection laws do not prescribe the allocation of commercial liabilities between the parties. Sophisticated companies usually slice and dice exposure in various ways in indemnification, limitation of liability, and warranty clauses. It is quite common to differentiate in risk allocation clauses based on whether customer and/or service provider contributed primarily to a breach or resulting harm, whether the service provider was in compliance with its contractual obligations, its information security policies, and applicable law, and whether a risk materialized that could have affected any other company, including the customer.
Myth 12: Customer Must Have the Right to Access the Provider’s Data Centers and Systems for Audit Purposes
Fact is that…
… customers need to reserve a right to audit the cloud service provider’s compliance measures
... the service provider may not let customers into its data centers or systems because that would impair the security of other customers’ data
… individual audits can be unnecessarily disruptive and costly
Possible compromise: Cloud service providers can arrange for routine, comprehensive audits of their systems by a generally accepted audit firm and make the results available to all customers.

If customers demand additional topics on the audit list, providers can expand the scope of the next scheduled audit, provided that the customers are willing to pay for the additional effort and the controls are within the scope of the service.
Questions