Original
Informatica Research
Publication

PRIVACY IN THE CLOUD:
IS IT GOOD ENOUGH?

Author:
Amalia Steiu
Enterprise Risk Advisor
Informatica Corporation

trust | informatica

INFORMATICA
INFORMATION SECURITY & RISK MANAGEMENT

1 Yonge St. Suite 1801
Toronto, ON. M5E 1W7
Tel: (416) 431-9012
InformationSecurityCanada.com
SecurityandPrivacy.ca

Summary

In an age of distributed accountability, the burden of ensuring the privacy of information assets now falls squarely on the shoulders of cloud service providers' business clients.

In the absence of legislation – but with the imminent arrival of standards - there are frameworks and tools that assist progressive organizations to obtain appropriate assurance that cloud service providers will adequately protect information privacy and thereby help offset the overall information risk.

Organizations pursuing value in the cloud must demand appropriate assurance as they build relationships with the cloud providers to allow them to manage, measure and monitor service levels for IT and compliance with privacy principles.

Table of Contents

1. Introduction 4

2. The Privacy Climate 4

3. Adequate Cloud Privacy 7

a) The 10 Privacy demands of the “trusting” organizations 7

b) Obtain Assurance of Privacy 8

4. References 9

1. Introduction

When Google announced in July 2010 that its public-sector-focused cloud computing service, Google Apps for Government, successfully completed a security certification and accreditation (C&A) process and received an authorization to operate (ATO) from the General Services Administration, it was very clear that they declared their compliance with the FISMA legislation (an attestation of U.S. federal government agencies's IT security). It meant that the federal government's General Services Administration had reviewed the documentation of Google's Cloud Computing Service security controls and issued an accreditation. No mention was made of any sensitive information being part of that assessment...

2. The Privacy Climate

In Europe, a large amount of resources is directed at data security and privacy assurance, to such a degree that some stakeholders are now calling for a global data protection law. It remains to be seen whether privacy and security standards and requirements can be harmonized enough to make such an ambitious proposal a reality, but as industry groups such as the Cloud Security Alliance routinely point out, the fact that the government approach to the cloud is as yet unclear — especially as to what the regulatory environment will look like — neither cloud service providers, technology vendors, nor government organizations (or even commercial enterprises) are going to be comfortable aggressively moving forward with cloud solutions.

There remain outstanding legal issues associated with cloud computing, especially in the area of privacy.

"Privacy concerns remain a significant impediment to the adoption of cloud computing for many potential customers. To ensure that society can maximize the benefits of cloud computing, removing the blockers around privacy is critical. Cloud service providers can start by building customers' confidence in the cloud. They can do this by demonstrating an inherent respect for privacy that is embodied in transparent business practices and a commitment to accountability." Brendon Lynch, Chief Privacy Officer, Microsoft

From a legal standpoint, it appears that while many opinions exist on how privacy can be protected in the cloud, who should ultimately be responsible for that protection, and how law enforcement agencies and other government entities should treat cloud environments among many discussion points. It appears that there are more unresolved issues than there are definite answers. There is no substantial case law that addresses general personal information stored in the cloud, which by its nature cannot necessarily be viewed analogously to data stored in file folders on hard drives owned or maintained by the parties to which the data belongs.

The willingness of people and businesses to put their information in the cloud is evidence that there is an expectation that privacy will be protected in the cloud, and such societal expectations have been factored into prior judicial decisions about expectations of privacy as other forms of technology matured and became pervasive. Courts should treat cloud service

providers as "virtual landlords" and narrowly apply third-party doctrine to data stored in the cloud.

European Union Regulatory Issues

Data protection authorities in the European Union are particularly interested in leveraging cloud computing, largely in response to inquiries from vendors and prospective users of cloud technologies but in such a manner as to ensure compliance with EU data protection requirements. Four primary legal cloud computing considerations in the E.U. include:

1. Data Controllers and Service Providers

In the European Union an entity's status is as either a “data controller” or a “data processor” and each such entity plays a unique role in the EU Data Directive. Data controllers determine the purposes and means of the processing of personal data and are responsible for compliance with data protection law, whereas data processors handle personal data on behalf of controllers. In anticipation of the changes to the EU Data Directive, we must mention that the Article 29 Working Party is seeking to give even more power and responsibility to data controllers.

With respect to cloud computing, an entity is viewed as a controller or a processor depending on the technical or architectural setup of the system or the type of cloud computing environment. This characterization will determine the liability of the respective parties for compliance with data protection obligations. *A controller remains responsible for data protection even where the data has been outsourced or transferred to a third party—including a cloud vendor—for processing.* It is therefore imperative for an organization interested in the cloud computing alternatives to undertake a rigorous assessment of its responsibility for the personal data processed by the cloud provider and, if applicable, enter into a data processing agreement requiring the cloud provider to act only according to the company's instructions, to ensure adequate technical and organizational security and privacy safeguards and otherwise to comply with legal requirements.

Viviane Redding, at the BBA Privacy event in June 2011, said: “Take the cloud, the story goes that the data in cross-border and cross-continent flows is impossible to regulate. This is not my vision of the future. I agree with those businesses arguing that regulation would be feasible if we make them more accountable! This is why I am considering the inclusion of the "accountability principle" in my reform so that data of citizens exported to third countries is always exported with their rights attached.”

2. Legal Bases for Processing Data in a Cloud

Under EU data protection law, organizations that “process” personal data must have a legal basis for doing so. Uploading data into the cloud is considered “processing” in the European Union. Before getting into complicated legal alternatives, a business most likely would rely on consent from the data subjects, contract fulfillment, or the “balance of interests” test when processing said data. But obtaining consent inevitably would be burdensome and in any case, raise significant legal issues in Europe. For example, to be valid under EU law, consent must be freely given, specific and informed. When it comes down to employment relationships,

however, under European data protection law, consent is not considered to have been "freely given". This is treated very differently in North America. To mitigate the uncertainty this creates, an organization could obtain individual employee consent as it notifies the relevant data protection authority of proposed processing. This process, however, could be so unpalatable as to outweigh the benefits of implementing a cloud-based computing solution.

3. Information Security Safeguards

E.U. data protection law requires that data controllers implement appropriate technical and organizational measures to protect personal data against

(1) accidental or unlawful destruction or loss;
(2) unauthorized alteration, disclosure or access (in particular where the processing involves the transmission of data over a network); and
(3) all other unlawful forms of processing.

These broad statements have full applicability to cloud computing environments and companies need to consider that the use of a cloud vendor increases the potential for unauthorized disclosure or access. It therefore becomes even more imperative that authentication and access safeguards be implemented with the utmost regard to providing an adequate level of security. Due to the high level of public access to the cloud, the risk of an information security breach and potential for information leakage is higher, therefore the cloud provider should be required by contract (if this wasn't their main concern towards their customers) to inform data controllers of any incidents with a potential for material data breaches.

4. Rights of Data Subjects

Privacy professionals know that the human right to privacy guarantees data subjects the legal right to access, block, rectify, delete and effectively control their individual data. Canadian Privacy Laws are deemed by the E.U. to uphold the European privacy standards and expectations. Due to the typical technical infrastructure details of a cloud computing environment, it may be difficult to guarantee that such requests for access, blocking, rectification, or deletion are effectively and properly managed. A service provider agreement, thoroughly crafted with the inclusion of effective controls would have to address this issue specifically. A cloud vendor will need to be certain that they can fulfill these obligations once they have been included as part of the agreement with a client, regardless of jurisdiction.

The Opportunity

Given the rapidly evolving legal stance on cloud privacy, providing guidance to companies venturing into the cloud is not a trivial matter. Legislatures and regulatory bodies around the world are grappling with the privacy and data security implications of cloud computing, but they have yet to promulgate any actionable requirements or recommendations. There is a void that can be exploited by both the Cloud Service Providers and the potential clients of cloud technology. The opportunity is on both sides to do right by the individuals. It is both feasible and beneficial overall, avoiding expensive re-engineering of privacy measures after the fact, when the law will inevitably mandate such controls.

3. Adequate Cloud Privacy

The two issues to be resolved are:

a) What is adequate cloud privacy, and

b) how can an organization gain assurance of such adequacy from the Cloud Service Provider (CSP)?

To solve the challenging set of issues stemming from these questions in the absence of legislative and regulatory guidance, we need to rely on best-in-class and Fair Information Principles.

There is no doubt that the "best in class" when it comes to privacy safeguards and regulations is the European Union. More so than the US, Europe has the track record to address control and management aspects related to a global cloud infrastructure. Europe thereby has the dubious de facto role of a technological and governmental practice leader.

Organizations seeking to use CSPs need to have a strong understanding of their own priorities and requirements around privacy before initiating a vendor relationship. Aside from inquiries into the overall risk governance structure of the CSP and their operating model, the prospective client must first be very specific about how their regulatory obligations and privacy assurance expectations must be met:

1. Define "breach" parameters and strict breach notification expectations, including the right of the client organization to audit under certain conditions. The EU Data Directive is going to mandate breach notifications.
2. Thorough reviews of encryption technologies and how confidentiality controls are implemented, including key management infrastructures
3. The client organization needs to know how de-identifiable their data really is, including who knows that one particular tenancy belongs to a specific client: as data custodians, IT staff can never know whose data they are managing and all activities on such data should be conducted as indirectly as possible.
4. The prospective client (or demand organization) needs to be very specific about data access to avoid incurring the incremental costs of frequent requests to access their own data.
5. Assurance terms with respect to data backup and recovery. What constitute disaster and recovery conditions, in particular service levels and guarantees for data integrity and confidentiality
6. Anticipation of CSP mergers and acquisitions and the risk mitigation plans clearly stated in the contract
7. Organizations will also need to be very clear about retention periods, where the data can or cannot be transferred, logging of access by administrators to cloud systems and the ability of other parties to access the data for market research or any other activities.
8. Geographic locations where the demand organization data could be held/located/distributed as well as third party suppliers to the CSP are paramount. The demand organization must carry out extensive due diligence to ensure the

enforcement of data privacy and security safeguards are strictly maintained regardless of the legislative and regulatory climate of the geographic area where data may reside.

9. The demand organization must create and share with the CSP their contract monitoring framework including monitoring privacy safeguards and obligations. The ability to monitor the adherence of cloud providers to contractual terms indicates a high level of risk and privacy maturity on the part of service providers. Are CSPs willing to accept certification responsibilities for compliance?
10. Set provisions for continuous improvement of privacy safeguards and controls. A trustworthy CSP will welcome the input of their clients (demand organizations) and will have a roadmap for improving privacy and security over time and as needed. Can the cloud solution meet future regulatory requirements? This is where the IPC's Privacy by ReDesign framework can provide immense value.

b) How to gain assurance of Privacy from a CSP: Canada benefits from high level and applicable methodologies that have at their core Fair Information Principles. The IPC (Ontario Information Privacy Commissioner's Office) has issued a guiding Privacy Impact Assessment document part of the internationally acclaimed Privacy By Design suite which provides high level guidance for privacy impact,

http://privacybydesign.ca/content/uploads/2011/06/2011-06-07-PbD-PIA.pdf

The guiding principles in this document may be used to understand processes associated with privacy assessment from a governance perspective. To provide executive-level reporting and technical completeness, demand organizations may employ custom methodologies, or opt for a proven approach such as the FlexSecure Verify™ Cloud Assessment solution from Informatica. Regardless of approach, the focus must remain on continuous visibility into cloud-based activities as they pertain to sensitive information over the duration of the CSP provisioning agreement.

4. References

1. NIST (The US National Institute of Standards and Technology) Special Publication 800-145, The NIST Definition of Cloud Computing

2. The European Commission's external report on risks and opportunities with Cloud Computing http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

3. Lisa Sotto, **Cloud Computing**, BNA Privacy & Security L. Report, 9PVLR 269, Feb. 15, 2010

4. Privacy and Data Security Risks in Cloud Computing, http://lawprofessors.typepad.com/law_librarian_blog/2010/02/privacy-and-data-security-risks-in-cloud-computing.html by Lisa J. Sotto, Bridget C. Treacy, and Melinda L. McLellan

5. Steve Ganz blog http://blog.securityarchitecture.com/2010/08/major-cloud-computing-privacy-legal.html

6. Ernst & Young, Top 11 Privacy trends in 2011 http://www.ey.com/GL/en/Services/Advisory/IT-Risk-and-Assurance/Top-11-privacy-trends-for-2011

7. Privacy by Design Privacy Impact Assessment, http://privacybydesign.ca/content/uploads/2011/06/2011-06-07-PbD-PIA.pdf

8. Viviane Reding EU Justice Commissioner, Press Release BBA (British Bankers' Association) Data Protection and Privacy Conference London, 20 June 2011 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/452&format=HTML&aged=0&language=EN&guiLanguage=en