ACT | The App Association

White paper on cloud privacy standard ISO 27018

The Importance of Cloud

Whether it's the world's largest insurance company, or the local PR consultancy, it is clear that cloud computing is big business. IHS estimates that global business spending on the cloud (infrastructure and services) reached $174.2 billion at the end of 2014, up 20 percent from 2013.[1] By 2017, that number is expected to reach $235.1 billion, triple what it was in 2011. Cloud is so critical that Gartner predicts by 2016 it will outstrip all other IT spending for the corporate world.

Cloud gives companies an efficient and inexpensive way to provide services and run their businesses. Cloud computing has allowed businesses to cut IT costs by over 35 percent,[2] as well as improving IT staff productivity, simplifying and standardizing infrastructure, launch revenue-generating services more quickly, and improve resource utilization.[3] 41 percent of director-level staff of 304 European organizations identified the cloud as a way to gain a business advantage.[4]

And it is not just tech companies who are using the cloud to get ahead. Industries such as banking, energy and utilities, healthcare providers, insurance, media, manufacturing, retail, and education report that they have incorporated cloud.

For small businesses, use of the cloud allows expansion of operations and reach beyond what would be possible if they had to individually set up their own infrastructure.[5] For example, a small business hosts a popular event and wants to stream that event online. It can acquire additional bandwidth from cloud servers during the time of the event rather than having to purchase expensive servers for bandwidth unnecessary to the business the rest of the year. The ability to, in real time, adjust physical infrastructure allows small businesses to take advantage of the economy of scale the cloud provides.[6]

Companies who have seen growth and cost savings from cloud are now asking the next logical question: how do their cloud service providers (CSPs) protect their data and their customers' data, especially in light of the number of high profile security breaches?

There is space in the market for a standard around cloud which would assist companies in choosing a CSP and ensure the best care and protection of their data.

ACT | The App Association
1401 K Street NW Suite 502
Washington, DC 20005

202.331.2130
@ACTonline
ACTonline.org
/actonline

Why A Standard?

While cloud has become ubiquitous in today's business environment, there has been little guidance in choosing the correct CSP for a business's needs: CSPs vary in the information they make available to potential customers about privacy protections and there is no guarantee that those promises are actually fulfilled. When comparing services, businesses are often left comparing apples to oranges. Now that the cloud market has matured, it is time for a systematic way to look at cloud privacy protections.

Standards help businesses looking for a CSP to find the one which works best for them by fostering transparency in practices and fostering trust in the stakeholders who participate in the review process. Businesses trying to determine the best CSP for their operations will benefit from increased clarity and better control over their data if they choose a provider who follows the standard.

Standards are also a benefit to CSPs, who can use participation in the standard to promote their privacy protections in a way that potential customers can understand. Now that there is so much information available about privacy (with a myriad of different terms used to define it) a standard helps establish common ground rules that everyone can follow and businesses can easily understand. Further, standards can have international reach. When any business competes in a global market, like CSPs, the ability to have predictable and understandable guidelines which extend across multiple jurisdictions is good for business.

A standard is the best way to provide clarity around privacy in the cloud because it is flexible enough to grow with technology and is built by technical experts who best understand cloud and its capabilities. With the cloud industry growing rapidly, a standard can more easily adapt and grow along with it.

What Standard?

The first international standard put forward to address this issue is ISO/IEC 27018.

ISO/IEC 27018[7] is a standard put forward by International Organization for Standardization (ISO) that creates the first voluntary international standard around business-to-business cloud computing services. ISO 27018 gives CSPs that act as processors a standard way to be transparent about their privacy practices and allow businesses to compare CSPs. In order to comply with the standard, participating CSPs must provide transparency in the following practices:

Customer Control over Personally Identifiable Information (PII) and absence of data mining for advertising purposes

Businesses trust CSPs with tremendous amounts of personally identifiable information (PII).[8] This information includes customer data and employee information. With such sensitive data, companies are interested in ensuring they retain control over that information when they place it in the cloud.

In order to be compliant with ISO 27018, a CSP must process PII only as instructed by the customer. PII cannot be used by the CSP for advertising and marketing unless express consent is obtained from the customer and it must be possible for a customer to use the service without having to consent that their PII will be used for advertising purposes. Further, even if permission is given, the CSP cannot process customer PII for any purpose independent of the instructions of the customer.

Transparent PII and Data Retention Policies

ISO 27018 also requires that CSPs be transparent about their practices. Each CSP under the standard must provide transparent PII and data retention policies as regards how data is handled and where it is stored. Importantly, CSPs must also provide a method for customers to extract their data or delete it after they leave the service.

List Third Parties

CSPs, like the vast majority of tech businesses, use third parties which specialize in specific functions in order to provide services to their customers at a reduced cost. These third parties, depending on what service they are providing to the CSP, could have access to PII that companies entrust to cloud processors.

ISO 27018 requires that CSPs adhering to the standard fully disclose all third parties who help process data and therefore have access to customer PII. This allows the companies to be better informed about who has access to their data and how they could use it.

Data Breach Procedures

With data breach so much a concern for companies today, ISO 27018 requires that, in the event of a security breach, the CSP must conduct a review to determine if there was any loss, disclosure, or alteration of PII. Further, the CSP must notify customers and keep clear records about the incident itself and the CSP's response to it.

The Future of Cloud Privacy Standards

Today, ISO 27018 provides a clear and transparent guidance for CSPs to promote privacy protections and allows businesses to make informed decisions about the cloud. CSPs that work to comply with the cloud help foster trust with their customers and advocate for best practices within their industry.

But even more than the guidance it provides today, ISO 27018 is a reference point on which future standards may improve. As the first international standard around cloud privacy, ISO 27018 starts a dialogue of how best CSPs can provide transparency about privacy and security. Future standards will use what the ISO has done as a start, building on lessons learned and innovations in the CSP industry. Businesses of tomorrow who will rely on the safety of their cloud data can look back at ISO 27018 as the start of an international dialogue about privacy in the cloud.

ISO 27018 is an important first step for protecting PII in the cloud. It is built on previous ISO guidance and will continue to evolve along with CSPs to provide more secure services upon which businesses can grow.

Endnotes

[1] "Cloud-Related Spending by Businesses to Triple from 2011 to 2017," HIS (February 14, 2014), available at http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017.
[2] "Cloud Computing Services – A Global Strategic Business Report," Global Industry Analysts, Inc. (August 2013) available at http://www.strategyr.com/Cloud_Computing_Services_Market_Report.asp.
[3] "Midsize Enterprises Leading the Way With Cloud Adoption," Cisco (last viewed January 27, 2015) available at http://share.cisco.com/cloudadoption/.
[4] Mike Wheatley, "Clear Skies Ahead: Half of Europe's Enterprises Dismiss the Cloud," Cloud Angle (September 11, 2014), available at http://siliconangle.com/blog/2014/09/11/clear-skies-ahead-half-of-euro-enterprises-dismiss-the-cloud/?angle=cloud.
[5] See Jonathan Godfrey, "Cloud Legislation Important for Small Businesses," ACT | The App Association (October 5, 2012) available at http://actonline.org/2012/10/cloud-legislation-important-for-small-businesses/.
[6] Kevin L. Jackson, "The Economic Benefit of Cloud Computing," Forbes (September 17, 2011), available at http://www.forbes.com/sites/kevinjackson/2011/09/17/the-economic-benefit-of-cloud-computing/.
[7] ISO/IEC 27018:2014, available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498.
[8] PII is defined in ISO 27018 as "any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal." ISO/IEC 27018:2014(E) Section 3.2