Storing Data in the Cloud and Data Residency Laws: Irreconcilable Differences?

For all its operational benefits, the cloud computing model that relies on distributed infrastructure to generate economies of scale presents a conceptual challenge to data residency legislation. Equally, for cloud service providers the business challenge is to deliver a similar level of flexibility and cost-effective service for customers in countries with stringent data residency requirements without having to build out datacenters in each jurisdiction. Cloud service providers store data all over the globe, and are constantly moving the data from one data center to the next for a host of reasons including cost and redundancy. Applying a set of constraints to the movement of data based on data residency requirements would introduce an additional layer of complexity that would erode cloud computing's value proposition.

However, multiple countries including India, Switzerland, Germany, Australia and Canada have enacted laws restricting corporations from storing data outside their physical country borders. For example, the EU Safe Harbor Principles mandates that companies operating within the European Union are forbidden from sending personally identifiable information (PII) outside the European economic area unless it is guaranteed that the data will receive equivalent levels of protection. And while growing concerns about the privacy of cloud data drive regulations elsewhere, national security concerns have driven the definition of US legislation that extends the ability of the federal government and law enforcement agencies to subpoena communications and emails stored in the cloud.

> Microsoft publicly admitted that any data stored or processed in Europe and other countries, including email, file storage and web application are liable for US government inspection under the US Patriot Act.[1]

The US is, however, not alone with regards to laws like the Foreign Intelligence Surveillance Amendments (FISA) Act or the USA PATRIOT Act. Many countries have comparable laws allowing them access to cloud-stored data outside their respective jurisdictions.

The current response to this challenge is to follow the lawful course of action, and store data within each jurisdiction (or simply not move to the cloud). For cloud service providers the cost and overhead are significant, reducing the overall gain of cloud storage. Additionally, with legislations such as FISA and the like, frequently this solution does not apply since the cloud service provider may be a US institution, or affiliate. At the heart of the concerns that bring residency under consideration is how organizations can continue to maintain control and protection of personal information, even when the information resides on a third-party service that relies on a distributed infrastructure to deliver resiliency, availability and flexibility to customers.

[1] *http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225*

Information Security and Data Protection Laws

The interaction between the evolution of information security and the definition of data protection mandates either by legislative bodies or industry groups is a dynamic one. By way of illustration, compliance requirements and data breach laws have been regularly updated as new information security alternatives (especially in the area of encryption) have been developed.

In the US, over 40 US states have breach notification laws mandating that if a company is aware of lost or stolen consumer PII, they are required to directly notify the consumer. When these laws were initially enacted (starting with the State of California in 2002), the laws generally stated that regardless of the circumstances, the company was required to notify the consumer.

However, the laws have gradually been amended and over 25 states have enacted an exemption for encrypted personal data. In instances where the lost or stolen data was encrypted, the company is not required to notify the consumer.

The following description of this landmark law is provided by the California Office of Privacy Protection:[2]

> "A business or a State agency that maintains unencrypted computerized data that includes personal information, as defined, [shall] notify any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The underlying argument for differentiating between unencrypted data and encrypted data in the context of breach notification requirements is that, in the instance where the data is encrypted, the attacker has gained access to useless gibberish if they do not hold the encryption keys. Encryption of the data is considered – in the eyes of the law – to constitute sufficient data protection even in the case of a successful data breach.

In the same vein, cloud computing is an evolving paradigm where both the obligations of the data owner, and acceptable forms of data protection are still in the process of initial definition. As cloud computing develops, gains popularity, and becomes an established method of data storage, the laws pertaining to cloud computing will continue to evolve in the same way that data breach laws have and continue to evolve.

By way of example, encryption is already recognized in the state of Nevada[3] as a means of securing data outside of geographic boundaries:

> "A data collector doing business in this State . . . shall not:
>
> (a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or
>
> (b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information."

It is apparent that the regulations are slowly moving towards encryption as a method of securing data and excluding encrypted data from data residency legislations.

[2] www.privacy.ca.gov/privacy_laws/index.shtml
[3] http://www.paulmudgett.com/resources/Nevada_Data_Security_Law.pdf

Emerging Approaches to Cloud Data Residency Regulations

While data residency regulations can be narrowly defined, in many jurisdictions the data residency laws can be interpreted as not to applying data that has been encrypted before being sent to the cloud.

Dr. Thilo Weichert, Head of the Independent Centre for Privacy Protection for the German state of Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein – ULD), when discussing applicability of data privacy laws in a paper called Cloud Computing & Data Privacy, argues the following:

> "Use of aliasing—replacing the identifiers for a natural person with other characteristics (BDSG § 3(6a))—does not necessarily mean that data privacy law is inapplicable. However, this method can make it so difficult to identify the data subject that the level of privacy is sufficient to permit data processing."

According to Dr. Weichert, if data is anonymized or sufficiently aliased to the extent that the identity of individuals is indecipherable, then data residency law does not apply. Encryption takes anonymizing and aliasing a step further, where the data is completely indecipherable and therefore should not be subject to data residency law.

Similarly, under the European Union's Data Protection Directive (EU DPD),[4] data residency should not present a legal obstacle as long as the data is encrypted.

When data is encrypted, PPI is completely unidentifiable and therefore encrypted data should not be subject to data privacy regulations.

> "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;"

Likewise, under Canadian privacy law, both federal bodies and commercial organizations domiciled within Canadian borders are responsible for the privacy and protection of personal information in their custody. This requirement applies regardless of where the data resides.

While significant concerns have been articulated with regards to the probability of disclosure to US law enforcement agencies of data that resides within datacenters located within the US, the requirements pertain directly to the safeguards in place to maintain control.

As noted in her formal response to a question related to compliance with the Freedom of Information and Protection of Privacy Act presented by two members of the Ontario provincial parliament about the privacy and security of personal information collected by the Ministry of Natural Resources that is currently being stored in the U.S., Ann Cavoukian, Information and Privacy Commissioner for the Province of Ontario wrote:

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

> "The critical question for institutions which have outsourced their operations across provincial or international borders is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. I have always taken the position that you can outsource services, but you cannot outsource accountability."

The pragmatic approach advanced by Commissioner Cavoukian can be articulated as: to the extent that the data owner retains the encryption keys, the location of the encrypted data is a secondary issue. If the encrypted data leaves the jurisdiction, but the keys remain under the data owner or controller's direct control, the level of protection can be understood to be sufficient in terms of data residency requirements. However, this model also implies that the data encryption scheme is maintained externally and independently of the cloud service provider's environment, and that data is encrypted before it is sent to the cloud.

Vaultive Persistent Encryption and Data Residency

For organizations with data residency concerns, Vaultive's persistent encryption ensures that data is never decrypted when resident in a third party's environment. Functioning as a gateway that can be deployed either on-premise, at a trusted third party or a within a dedicated VPN, the Vaultive appliance can serve as a demarcation point between the cloud and the network subject to data residency requirements.

The data is encrypted as it leaves the trusted network and traverses the gateway. Because the organization's IT department retains control of the encryption keys, the data is never decrypted while processed in the cloud.

Once encrypted at the boundary of the trusted network, the data remains encrypted, even when processed within the cloud service provider environment. Regardless of the jurisdiction where the data resides, control of the access to the data remains with the organization that retains the encryption key. Control of the keys in combination with Vaultive's encryption across the data lifecycle – in transit, at rest and in use – provide the foundation to satisfy requirements for control and adequate safeguards for the privacy of personal information.

Although the encrypted data may leave the physical borders of the country in which your corporation resides, the data is encrypted while outside of your jurisdiction. The keys are retained within your corporation's legal jurisdiction and therefore, the data cannot be accessed or read until it returns to the physical borders in which your organization resides and can be decrypted with the keys.