C-Suite Primer on Data Sovereignty & Data Custody: What You Need to Know

Executive Summary

It has been almost a year since former NSA contractor Edward Snowden released a trove of documents revealing the large-scale collection, analysis, and storage of personal data on U.S. citizens and foreigners – much of it out of the data centers of telecommunications, Internet, and cloud service providers. In the year since, you most likely have heard about the concepts of "data sovereignty" and "data custody." You might have heard them in your boardroom.

Data sovereignty is the question of which sovereign's (i.e., country's) laws govern your data. The concept is often taken to mean that your data is subject to the laws of the country in which it is located, but that may not be the case; data sovereignty may instead mean that the data is subject to the laws of the country in which it originated, or the laws of the country in which the cloud provider is headquartered. In the cloud, data sovereignty can become an issue because different countries have different laws governing the collection, use, storage, and transmission of data within their borders. Data custody is about who controls your data; essentially, who has the right – or the obligation – to hand it over if the government comes knocking.

This whitepaper details what data sovereignty and data custody mean for the C-level enterprise executive. Whether your focus is on growing the business, or keeping it secure, or managing IT, it is imperative to understand the key issues addressed in this whitepaper. Here's why: If you don't know where your data is, and if you don't know who controls it, you're putting the security of your enterprise data, and your customers' data, at risk.

If you don't know where the servers that hold your data are, you don't know whose rules you might be beholden to. And if you don't know (or can't control) whose rules you might be beholden to, you can't know whether the jurisdictional laws in that location are in sync with your corporate policies (and your own sovereign's data laws). You're risking non-compliance, or worse.

Yet if your data is in the typical public cloud, the likelihood is very small that you even know where your data is, much less have control of it.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

The Solution: See and Control Your Data – Where It Is and Who Has Access to It

Addressing critical data sovereignty and data custody issues is about making fully informed business decisions. Decisions about which locations you want IT infrastructure in, and which you don't. About which infrastructure model best suits both your needs and the data sovereignty and data custody particulars of the location. About what kinds of security processes and due diligence procedures to put in place.

Making those fully informed decisions requires that you answer the following questions:

Are the jurisdictional laws in the given location in sync with your corporate policies and your sovereign's data laws? If the answer to that question is no, you may not want IT infrastructure in that location, or you may want to operate under tighter control with more robust security than you might otherwise deploy. In this case, your best IT infrastructure solution might be on-premises or off-premises (a.k.a., any-premises) private cloud and end-to-end encryption to secure the data in transit.

Is your cloud provider capable of accommodating the laws of the countries in which you do business? If the answer to that question is no, and you want to do business in that given location, you'll have to figure out how to comply with the local laws. In this case, your best IT infrastructure solution might be colocation in a local data center or any-premises private cloud.

Do any of the locations in which you do business require you to keep their citizens' data in-country? If the answer to that question is yes, and you want to do business in that given location, you have to figure out a way to keep the data in-country. In this case, your best IT infrastructure solution might be colocation in a local data center or any-premises private cloud.

Are you prepared to protect enterprise data and government data even in the face of surveillance programs that you're not aware of? Without knowledge of the programs the government is running, it's impossible to make informed business decisions. So in the face of potential secret programs, pre-emptive measures may be necessary. In this case, your best IT infrastructure solution might be any-premises private cloud and end-to-end encryption to secure the data in transit.

Do you know, and are you comfortable with, what your cloud provider would do if the government of any of the countries in which your enterprise data is running or stored asked it to turn over your data or your encryption keys? There are many reasons an enterprise would decide to go to the public cloud. But there are risks that must be accounted for and mitigated. In this case, your best IT infrastructure solution might be public cloud after rigorous due diligence, where you control the encryption keys – or any-premises private cloud.

Do You Need to Read this Whitepaper?

Pop Quiz - Check All That Apply

☐ I know where my enterprise data is, including the data running in cloud applications and stored on cloud infrastructure. Where it is physically. As in, its GPS coordinates. *At this moment.*

☐ In all of the countries I do business in, I am aware of – and can accommodate – obligations to keep customer data only within that country's borders.

☐ If the government of any of the countries in which my enterprise data is running or stored asked my cloud provider to turn over my data or my encryption keys, I know and am comfortable with what my cloud provider would do.

Making fully informed IT infrastructure decisions requires the ability to see and control where your data is and who has access to it. In this whitepaper, you'll gain the insight you need to answer the questions listed above for your specific circumstances. And then to take those solutions to the boardroom.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

C-Suite Primer on Data Sovereignty & Data Custody: What You Need to Know

Data Sovereignty & Data Custody: What They Mean for the Enterprise

It used to be that you could have your IT infrastructure one of two ways: on premises in a data center you built, owned, and managed; or colocated inside a data center built, owned, and managed by someone else. Today, it's a brave new world. You still have the on-premises and colocated options, but you can also have IT infrastructure delivered as-a-service in the cloud. That cloud can be public, private, or hybrid (some combination of both). With some cloud providers, you can have a private cloud on any premises, anywhere in the world.

There's no question that the proliferation of IT infrastructure options is key to our ability to manage the ever-increasing amount of data we generate and consume. But all these options, and the global nature of them, make IT management much more complicated than it was in that not-too-distant past. When your IT infrastructure is located on your premises or colocated with a data center provider, there's no question where your data is. You have the key to the cabinet; the answer to the question "Who has custody?" is easy – it's you.

But when your data applications or infrastructure – even some of them – are in the cloud, it can be difficult or impossible to say where in the world your data resides, much less where it has been. (That is data sovereignty.) The amount of control you have over your data depends on the laws of the country where it is, and the policies of the cloud service provider. (That is data custody.)

While these are not new issues, the rising ubiquity of cloud computing and Edward Snowden's revelations of U.S. National Security Agency (NSA) data surveillance have brought the conversation about data sovereignty and data custody into the boardroom. Enterprise leaders overwhelmingly understand the importance of location when it comes to storing company data, and many have taken or are planning new action to protect the privacy and security of their data.

Yet the fact remains that data sovereignty and data custody present legitimate challenges for global enterprises. And those challenges are not going away.

Have the Snowden Revelations Changed Your Approach to the Cloud?

95% of ICT decision makers believe location matters when it comes to strong company data

88% are changing their cloud buying behavior

84% feel they need more training on data protection laws

52% are carrying out greater due diligence on cloud providers than ever before

38% are amending their procurement conditions for cloud providers

31% are moving data to locations where the business knows it will be safe

Source: NTT Communications, March 2014

1.866.437.4518
io.com
info@io.com
@ioDataCenters

C-Suite Primer on Data Sovereignty & Data Custody: What You Need to Know

The Issues

Data Sovereignty: Whose Laws Apply?

Data sovereignty is the question of which sovereign's laws govern your data.[1] Michael Chertoff, former Secretary of the U.S. Department of Homeland Security, explains the issue well: "While the location of a data storage center may be irrelevant to many operations and applications, the physical location of a piece of data or information is often critical in determining which sovereign nation controls that data. **Indeed, if information is power, then the location of information may determine who exercises power in cyberspace.**" [2]

Data sovereignty can become an issue because different sovereigns (i.e., countries) have different laws governing the collection, use, storage, and transmission of data. But whose laws apply? As Chertoff asks, is it "The law of the country where the customer created the data? The law of the country (or several countries) where the server(s) are maintained? Or the law of the home country where the data storage provider is headquartered? Or all of the above?" [3]

The "whose laws apply" question is so difficult to answer in part because of the number and range of sovereign data laws around the world. More than 100 national and state governments have enacted data privacy and disclosure laws.[4] Among them are:

Argentina
Personal Data Protection Act, Information Confidentiality Law

Australia
National Privacy Principles, State Privacy Bills, Email Spam and Privacy Bills

Brazil
Article 5 of Constitution

Canada
Personal Information Protection and Electronic Documents Act, Freedom of Information and Protection of Privacy Act, Personal Information Protection Act

Chile
Protection of Personal Data Act

European Union
EU Data Protection Directive, State Data Protection Laws

Europe
Privacy laws in 28 countries

Hong Kong
Personal Data Privacy Ordinance

India
Information Technology Act

Japan
Personal Information Protection Act

Mexico
Personal Data Protection Law

New Zealand
Privacy Amendment Act

South Korea
Network Utilization and Data Protection Act

United Kingdom
Information Commissioner's Office (ICO) Privacy and Electronic Communications Regulations

U.S. Federal
HIPAA & HITECH, Privacy Protection Act, Right to Financial Privacy Act of 1978 (RFPA), Safe Harbor, Patriot Act

U.S. States
Breach notification in 39 states

[1] A sovereign is "a group or body of persons or a state having supreme authority." In most cases, the word is synonymous with "country."

[2] Michael Chertoff, "Data Sovereignty in the Cloud: The Issues for Government," SafeGov.org, Nov 2011.

[3] Ibid.

[4] Not an exhaustive list. This is instead design to show the number and range of sovereign laws governing data. Source: CipherCloud, "Managing Data Residency and Compliance in the Cloud Age."

1.866.437.4518
io.com
info@io.com
@ioDataCenters

Leading enterprises are now wise to the fact that this tangled web of national and state laws governing the use, storage, and transmission of data makes compliance in the cloud very difficult. The issue is particularly acute for enterprises in highly regulated industries like financial services and health care. As Andrew Stokes, Chief Scientist of Deutsche Bank Global Technology, says, "There are so many regulators and regulations – we need to be safe. Every geography has its own unique sectors and laws."

Sometimes the laws that apply are less "friendly" than your own sovereign's laws, putting enterprise data and customer data at risk. In other cases, the laws are significantly more strict, requiring levels of privacy protection, for example, that your cloud provider may not be equipped to accommodate. International agreements such as the Convention on Cybercrime from the Council of Europe arose to address the variation of laws governing digital information around the world. But not every country is party to those agreements.

So one issue is the difficulty of navigating these different (and sometimes conflicting) laws. But even doing that depends on knowing – and controlling – where your data is. If you don't know where the servers that hold your data are, you don't know whose rules you might be beholden to. And if you don't know (or can't control) whose rules you might be beholden to, you can't know whether the jurisdictional laws in that location are in sync with your corporate policies and your sovereign's data laws.

To complicate matters (as if), when you're in the cloud, the likelihood that your data will stay in one physical location is nil. And when your data changes cloud locations, the laws it is subject to change also. "Essentially, data is subject to the laws of the legal jurisdiction in which the cloud that hosts it is located, wherever that may be *at any given time*."[5]

In fact, many of the benefits of the cloud are based on the premise that data is moved swiftly between data centers as cloud providers distribute workloads in order to optimize the capacity and efficiency of their servers, and to create better resiliency for business continuity of operations. Yet "the ease with which cloud resources can be allocated and reallocated makes it more likely that it will be done without an appropriate review of the relevant legal issues."[6]

What Happens Here Stays Here?

Foreign countries – including Europe, Australia, New Zealand, Brazil, and a number of countries in Asia – are increasingly passing laws that require that data generated within their borders stay within their borders. Why? Because when the data of one country's citizens leaves its borders, the country loses the ability to regulate the use of that data. In 2006, for example, when European leaders learned that the U.S. was surveilling SWIFT financial transaction data of European citizens, they passed laws requiring SWIFT to keep European citizens' data on servers in Europe – out of the reach of the United States.[7]

For many enterprises, the cloud is a way to have a data center "presence" everywhere they do business. But if data generated in one country of the many you do business in is required to stay in that country, will your cloud provider be willing – or able – to abide? When the answer is no, some suggest that the enterprise seek a local cloud provider. But due diligence can be difficult from across the ocean, and the capabilities and data custody practices of nascent cloud providers – especially in emerging markets like Asia and Latin America – are not yet clear.

When government regulations governing data are known, then enterprises can make informed decisions about where to locate their IT infrastructure, and with whom. Most governments, for example, have published laws on data retention and personally identifiable information. **As long as the enterprise's cloud solution gives the enterprise the capability to know and control where its data is, then the enterprise can make cloud location decisions based on its knowledge of prevailing rules.**

PRISM

When government programs are secret, however, informed decision making is not possible. That was the case with the NSA's secret surveillance program, PRISM, which was unveiled in 2013 by former NSA contractor Edward Snowden. PRISM was arguably legal in the United States. But because it was a secret, enterprises couldn't consider it as a factor when making decisions about where to locate their data operations.

[5] CFO Handbook, "Conquering the Cloud," 2012.

[6] QMUL Cloud Computing Project, "What is Cloud Computing?" Queen Mary University London, 2010.

[7] Michael Chertoff, "Data Sovereignty in the Cloud: The Issues for Government," SafeGov.org, Nov 2011.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

Avoiding that kind of secret government surveillance program, however, is complicated. And while other countries did a lot of chest thumping after PRISM was revealed, there is no doubt that most countries have surveillance programs. In other words, complete data security may be impossible for an enterprise to guarantee through location decisions alone. Certainly part of the solution is locational – the enterprise must have the ability to know and control where its digital data is. But end-to-end encryption is also critical. Both of these issues are discussed with more depth later in this white paper.

Data Custody: Who Controls the Data?

Beyond geographic location, who is managing the infrastructure that stores your data and runs your applications certainly matters because you have outsourced performance, security, and governance to that provider. But it also matters from a data custody perspective. To put it bluntly, if a government comes knocking with a subpoena, will the service provider hand over the keys?

"What are the implications of exposing data held offshore, or under the control of offshore entities, to examination by foreign law enforcement regimes or litigants?" [8]

The United States government (among many other governments, to be sure) accesses digital data for national security in many ways. The U.S. does so largely under the auspices of the PATRIOT Act, passed in 2001 in the wake of the September 11th terrorist attacks and designed to "provide the appropriate tools required to intercept and obstruct terrorists."

It was under the PATRIOT Act, for example, that the U.S. Foreign Intelligence Surveillance Court required Verizon, AT&T, Sprint, and presumably others to provide the FBI and NSA the metadata from millions of phone calls. That is just one example of the legal obtainment of data from private companies by U.S. government agencies. And while Americans may generally accept the PATRIOT Act's security/privacy tradeoff, citizens of other countries may feel differently.

At the end of the day, a government subpoena is a government subpoena, and an enterprise can't avoid responding to it any more than a cloud provider can. But most enterprises would prefer to respond to such government requests or demands on their own. Yet some cloud providers take up that response themselves, handing over encryption keys to client data. As CipherCloud's Michael Higashi argues, "Cloud application providers may hand the information over more easily than your organization would." [9]

Depending on the country's laws, cloud providers may be *obligated* to hand over your data. Furthermore, says Michael Snowden, Managing Director of OneNet (no relation to former NSA contractor Edward Snowden), "if you have a commercial conflict, your opponent's access to your digital data will depend upon the discovery rules applicable to the country in which your data is held."[10] So when it comes to data custody in the cloud, it is critical to know:

1) What the cloud provider's practice (and legal obligation) is if the government subpoenas your data
2) Whether the provider's practice (or obligation) is to inform you of such government requests
3) If a commercial conflict arises, what are the local laws governing the discovery of your digital data

[8] Cyberspace Law and Policy Centre, UNSW Faculty of Law, "Data Sovereignty and the Cloud- A Board and Executive Officer's Guide" Jul 2013.

[9] Michael Higashi, "Top 5 Best Practices to Eliminate Cloud Data Sovereignty Concerns," 20 Sep 2013.

[10] OneNet, "Why data sovereignty matters," 5 Nov 2013.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

The Solution: See and Control Your Data – Where It Is and Who Has Access to It

Addressing the data sovereignty and data custody issues described here is about making fully informed business decisions. Decisions about which locations you want IT infrastructure in, and which you don't. About which infrastructure model best suits both your needs and the data sovereignty and data custody particulars of the location. About what kinds of security processes and due diligence procedures to put in place.

> **"As part of any migration to the cloud, enterprises need to ensure they are aware of and comfortable with the locations where the data will be stored and the legal implications associated with those locations."** [11]

The following section provides a framework for the sorts of business decisions an enterprise will face with each data sovereignty and data custody issue, and the solutions that the enterprise should consider.

A Framework for IT Infrastructure Decision Making in the Context of Data Sovereignty and Data Custody Issues

Issue	Business Decision	Solutions
Are the jurisdictional laws in the given location in sync with your corporate policies and your sovereign's data laws? (Typically applies when the laws are "less friendly" than your own sovereign's laws, potentially putting enterprise data and customer data at risk.)	If the answer to that question is no, you may not want IT infrastructure in that location, or you may want to operate under tighter control with more robust security than you might otherwise deploy.	On-premises or off-premises (a.k.a., *any*-premises) private cloud *and* End-to-end encryption to secure the data in transit
Is your cloud provider capable of accommodating the laws of the countries in which you do business? (Typically applies when the location's laws are stricter than your own sovereign's laws, requiring higher levels of privacy protection, for example.)	If the answer to that question is no, and you want to do business in that given location, you'll have to figure out how to comply with local laws.	Colocation in a local data center *or* Any-premises private cloud
Do any of the locations in which you do business require you to keep their citizens' data in-country?	If the answer to that question is yes, and you want to do business in that given location, you have to figure out a way to keep the data in-country.	Colocation in a local data center *or* Any-premises private cloud

[11] Liam Tung, "Cloud security challenges go all the way to the board," ZDNet, 14 Apr 2014.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

Issue	Business Decision	Solutions
Are you prepared to protect enterprise data and government data even in the face of surveillance programs that you're not aware of?	Without knowledge of the programs the government is running, it's impossible to make informed business decisions. So in the face of potential secret programs, pre-emptive measures may be necessary.	Any-premises private cloud *and* End-to-end encryption to secure the data in transit
Do you know, and are you comfortable with, what your cloud provider would do if the government of any of the countries in which your enterprise data is running or stored asked it to turn over your data or your encryption keys?	There are many reasons an enterprise would decide to go to the public cloud. But there are risks that must be accounted for and mitigated.	Public cloud *and* Rigorous due diligence *and* You control the encryption keys *or* Any-premises private cloud

IT Infrastructure Solutions to Address Data Sovereignty and Data Custody Issues

As the framework above makes clear, there is no single IT infrastructure model that is always the best solution to data sovereignty/data custody issues. Discussed below are the various IT infrastructure models and the ways that they do or do not mitigate data sovereignty/data custody risks.

Local Public Cloud

Rising concerns about data sovereignty and data custody have led to regionalization of IT infrastructure on two fronts. First, in response to growing data sovereignty concerns, many enterprises are regionalizing their cloud infrastructure. That's especially true for non-U.S. enterprises now wary of hosting their data on U.S.-based infrastructure. "Enterprises in China and the Asia-Pacific region in particular appear to be more apprehensive about U.S. service providers and technology since the NSA disclosures. Many are expected to start looking at regional and local options for [cloud service]."[12]

In addition, partly as a response to rising concerns abroad about data sovereignty, some U.S.-based cloud service providers are setting up operations in different regions of the world, explains Gartner analyst Lawrence Pingree. (Regionalization can also lower delivery costs and improve performance for local customers.) "A lot of cloud and SaaS providers are regionalizing to improve agility and performance. The heightened attention on security issues will likely further speed the use of regional centers."[13]

Public cloud providers like Amazon Web Services and IBM, for example, have announced plans to build cloud facilities in farther-flung locations like China, India, the Middle East, and Africa.[14] While these cloud providers might be physically local in those countries, it's not clear how well U.S.-based cloud providers will really understand the local data sovereignty and data custody laws. Nor is it clear whether they will be considered by local law to be local or whether, because they are U.S.-based, they will still be considered U.S. entities subject to U.S. government subpoena.

[12] Jaikumar Vijayan, "Cloud computing 2014: Moving to a zero-trust security model," Computerworld, 31 Dec 2013.

[13] Jaikumar Vijayan, "Cloud computing 2014: Moving to a zero-trust security model," Computerworld, 31 Dec 2013.

[14] Brandon Butler, "Watch out Amazon: What IBM's $1.2B cloud investment really means," Network World, 17 Jan 2014.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

Custody Assurance

If the enterprise decides to use public cloud as part of its IT infrastructure model, the cloud provider's data custody policies are an essential element to consider. In its most recent "Who Has Your Back?" report, the Electronic Frontier Foundation (EFF) assesses companies' practices and policies against a set of data custody-related criteria.[15] The EFF suggests four questions that you should ask any cloud provider you're considering doing business with:

1) Do you **require the government to obtain a warrant** supported by probable cause before you will hand over the content of user communications?

2) Do you **tell users when the government seeks their data** (unless prohibited by law)? This gives users a chance to defend themselves against government demands for their data.

3) **Do you publish transparency reports** (e.g., statistics on how often you provide user data to the government)?

4) **Do you publish law enforcement guidelines** (policies or guidelines explaining how you respond to data demands from the government)?

The 2013 "Who Has Your Back" report concludes, "While we are pleased by the strides these companies have made over the past couple years, there's plenty of room for improvement." For example, "Amazon holds huge quantities of information as part of its cloud computing services and retail operations, yet does not promise to inform users when their data is sought by the government, produce annual transparency reports, or publish a law enforcement guide."[16]

Using a local public cloud provider *could* be a way to ensure compliance with local regulations, and/or to ensure that data created in a particular country stays within that country. Except that most public cloud offerings don't provide visibility into and control over where the data is and who has access to it. As the Snowden revelations have demonstrated, even the kind of data that might be considered non-critical – like email, for example – often still falls under the veil of assumed protection. And when that data is breached, the customer fallout can be incredibly damaging to the enterprise.

In a range of cases, even public clouds with the most robust encryption methods and most stellar transparency records simply don't offer the control and visibility necessary to resolve the data sovereignty and data custody issues discussed here. While encryption and provider assurance can mitigate data custody issues, and regionalized public cloud centers can help mitigate data sovereignty issues, the public cloud by its nature does not give the enterprise visibility or control. **The distributed, shared nature of public cloud runs counter to the visibility and control that many enterprises need to have over where there data is.**

On-premises or Off-premises (a.k.a. Any-premises) Private Cloud

According to a 2013 survey by the IT association CompTIA, 25 percent of enterprises are shifting from a public cloud to a private cloud solution.[17] Private cloud, which is implemented behind an enterprise's firewall, under control of the IT department, can be on-premises or off-premises. In other words, it can be located at your location, or inside a colocation provider's data center. Either way, it's behind your firewall and you retain control. Which means that you need resources on-site to manage the IT infrastructure. And you still have to navigate local laws governing the collection, storage, and use of data.

Private cloud IT infrastructure need not be in the form of a legacy data center – i.e., a custom-constructed data center. When the infrastructure is modular – purpose-built, standardized manufactured data center units – it can be deployed in a fit-for-purpose footprint on any premises, anywhere in the world. As a completely stand-alone, secured "box" with direct connect to the enterprise's ISP, the modular data center can be easier to defend even than a rack of private cloud infrastructure hosted in a data center – especially with a bulk encrypter on the cables at the inside edge of the module.

[15] Electronic Frontier Foundation, "Who Has Your Back? 2013" April 2013.

[16] Ibid.

[17] CompTIA, "4th Annual Trends in Cloud Computing," 5 Sep 2013.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

A modular private cloud with bulk encrypter allows the enterprise to control the geography in which it operates and, in the process, control which laws apply to its data. It solves for both known data sovereignty and data custody issues, at the same time protecting against threats from malicious actors. When the cloud is controlled by a true data center operating system it can be integrated with the enterprise's other IT infrastructure around the world to be globally interoperable.

That isn't just our opinion. In a 2013 report on cloud security, the U.S. Department of Defense (DoD) espouses on-premises private cloud for the security it enables. The report makes clear that to easily deploy a private cloud solution across geographies, modular infrastructure should be considered: "The task force recommends that DoD design, implement, and deploy a set of geographically distributed data centers that could be could be operated as a single system. A few tens of such consolidated cloud computing data centers, established across the United States and around the world, seems like a good start at creating a sensible cloud capability for DoD. **If appropriately designed, a collection of modular data centers would provide DoD with robust and elastic computing capacity.**"[18]

Colocation in a Local Data Center

Like using a local cloud provider, colocating IT infrastructure at a local data center could be a way to ensure compliance with local regulations, and/or to ensure that data created in a particular country stays within that country. Unlike using a local cloud provider, colocation doesn't enable the enterprise to leverage the benefits of the cloud. And, you must have local IT resources to manage your colocated infrastructure.

If considering colocation at a local data center, ask:

1) Is the data center-as-a-service provider mature enough to meet the enterprise's standards?

2) Does the provider offer data custody assurance? (Here, ask the same questions – above – that you'd ask of a local cloud provider.)

3) Do you have the ability to integrate control and monitoring of your data at that location with your other data around the world? (If not, you're creating silos.)

End-to-end Encryption to Secure the Data in Transit

Whatever IT infrastructure model the enterprise deploys, robust data encryption is a vital part of a secure cloud. For one, end-to-end bulk encryption prevents security agencies or others from tapping into backbone fiber optic cables and retrieving readable data. For example, Google, which had previously not encrypted data between its data centers, has installed bulk encrypters at the edge of every Google data center.[19] Security agencies could still tap the fiber, but wouldn't be able to read the data without the encryption key. Yahoo has announced plans to do the same.

Beyond bulk end-to-end encryption, it is important that the enterprise – not the cloud provider – retain control over encryption keys. As Gartner explains, "in a well-architected system, the cloud application provider does not have direct access to the keys. In this way, if a legal request is made for access to the data, the enterprise must be involved."[20]

Still, encryption only goes so far. It answers some data custody questions, such as: Can security agencies or other entities gain secret access to the data? If the government comes knocking with a warrant, can the cloud provider hand over the data, or is the enterprise the only entity with the keys? But it does not address the issue of data sovereignty, i.e.: Under whose jurisdiction is the data?

A Global IT Infrastructure Platform

In considering the range of available IT infrastructure solutions to address data sovereignty and data custody issues, it becomes clear that the enterprise IT infrastructure model of the future is one in which decisions are made based on a wide range of factors, including data sovereignty and data custody decisions.

[18] Department of Defense, Defense Science Board, "Cyber Security and Reliability in a Digital Cloud," Jan 2013.

[19] InfoSecurity Magazine, "Google Encrypts Connections Between its Servers," 25 Mar 2014.

[20] Gartner, "Five Cloud Data Residency Issues That Must Not Be Ignored," 26 Dec 2012.

1.866.437.4518
io.com
info@io.com
@ioDataCenters

The risk with that kind of fit-for-purpose, locate-anywhere model is that enterprise IT infrastructure becomes a patchwork of siloed, non-interoperable resources. Some custom-built, one-off data centers of different vintages, colocation through different providers around the world, cloud services from a range of vendors.

Guarding against that kind of data center patchwork requires an IT infrastructure platform that enables the enterprise to make infrastructure decisions that are optimized around each geography's data sovereignty and data custody particulars – leveraging a combination of the solutions described above as it makes the most sense in each location. When that best-fit IT infrastructure is part of a platform, it's globally interoperable.

Visibility and Control

Critical to the platform, and to all of the solutions listed above, is the ability to see and control where data is running and where it is stored – and who has access to it – at every location. That visibility and control is essential for the enterprise to be able to make fully informed decisions.

"CIOs want to see and control their data, down to the rack-level. Most public cloud deployments don't offer their end-user visibility into where their data resides. In 2014, enterprise CIOs will look at providers who offer visibility and controls that enable policy-based compliance with respect to domain. Whether it's corporate security standards or driving compute efficiency, the CIO will be expected to know where data resides and where specific applications are running at all times." [21]

Global visibility and control requires a true data center operating system, or DCOS. Sometimes referred to as the same as data center infrastructure management, or DCIM, a true data center operating system actually goes far beyond monitoring and reporting of data center assets to include control and automation. A single, global data center operating system enables visibility into and control over all IT infrastructure around the world.

451 Research explains that data center operating systems "can provide real-time 'live' information by constantly checking operational data. They can (usually) also detect and provide immediate notification of problems such as equipment failures, hotspots or issues with power distribution. Alarms and data about separate events can be correlated so managers can readily determine the root cause(s) and which equipment has been affected."[22]

[21] George Slessman, "2014: The Year the Data Center Will Rule," Wired, 6 Dec 2013.

[22] 451 Research, "Prefabricated Modular Datacenters: 2014 and Beyond," Dec 2013.

The Bottom Line

Where your data is matters. *Who* controls your data matters. Given those facts, addressing critical data sovereignty and data custody issues is about making fully informed business decisions. Decisions about which locations you want IT infrastructure in, and which you don't. About which infrastructure model best suits both your needs and the data sovereignty and data custody particulars of the location. About what kinds of security processes and due diligence procedures to put in place.

When you can check all the boxes below you can be confident that you know where your data is, and who controls it.

- ☐ I know where my enterprise data is, including the data running in cloud applications and stored on cloud infrastructure. Where it is physically. As in, its GPS coordinates. *At this moment.*

1.866.437.4518
io.com
info@io.com
@ioDataCenters

- ☐ In all of the countries I do business in, I am aware of – and can accommodate – obligations to keep customer data only within that country's borders.
- ☐ If the government of any of the countries in which my enterprise data is running or stored asked my cloud provider to turn over my data or my encryption keys, I know and am comfortable with what my cloud provider would do.

When you can check all those boxes, you can be confident in the security of your enterprise data, and your customers' data. You'll know – and be able to control – whose rules you are beholden to. With full visibility and control into where your data is and who has access to it you can confidently make the best IT infrastructure decisions for the business.

About IO

Founded in 2007, IO is a worldwide leader in software defined data center technology, services and solutions that enable businesses and governments to intelligently control their information.
To learn more, visit io.com or call 866.437.4518.

1.866.437.4518
io.com
info@io.com
@ioDataCenters