451 Research® | Advisory

DATA PRIVACY IN THE CLOUD

FIVE CURRENT ISSUES IN COMPLIANCE

Guidance for the IT Professional

A Report Commissioned by:

OPENTEXT™

MAY 2015

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

New York
20 West 37th Street, 6th Floor
New York, NY 10018
Phone: 212.505.3030
Fax: 212.505.2630

London
Paxton House (5th floor), 30 Artillery Lane
London, E1 7LS, UK
Phone: +44 (0) 207 426 0219
Fax: +44 (0) 207 426 4698

San Francisco
140 Geary Street, 9th Floor
San Francisco, CA 94108
Phone: 415.989.1555
Fax: 415.989.1558

Boston
1 Liberty Square, 5th Floor
Boston, MA 02109
Phone: 617.275.8818
Fax: 617.261.0688

TABLE OF CONTENTS

INTRODUCTION

The collection of technologies known as cloud computing have created revolutionary change in the way people around the world live and work. The 'cloud effect' on commerce has been impressive, with international business benefiting from the technological and cost efficiencies of cloud infrastructures. However, emerging and disruptive technologies rarely come without challenges and the need to navigate around potential risk. Cloud computing is no exception.

Although cloud computing has blurred borders from a technological standpoint, it has helped create greater divisions between nations from the legal and regulatory perspectives. Whether because of political fallout from the NSA-Snowden controversy or consternation over corporate data-collection practices, there has been a global backlash against the unbridled use of individuals' personal data. From the European Union to Brazil and beyond, political events have been catalysts for more stringent data-privacy laws, but these laws go beyond the protection of personal data. Legislative initiatives such as data localization may protect data, but they may also hinder the technological advances cloud computing is supposed to bring.

Although cloud computing has blurred borders from a technological standpoint, it has helped create greater divisions between nations from the legal and regulatory perspectives.

Cloud computing offers tremendous possibilities for global businesses, but to capitalize on these opportunities, IT professionals need to have a familiarity with data-privacy-compliance issues. With this this need in mind, this report examines five current data-privacy issues: the Microsoft Dublin warrant controversy, international e-discovery and e-disclosure, the US-EU Safe Harbor Framework, the pending EU General Data Protection Regulation, and the expansion of data-privacy laws around the world. IT professionals don't need to become lawyers, but IT teams with a basic understanding of these issues – their backgrounds and why they matter – can be instrumental in preventing data-privacy-compliance failures as they prepare their cloud strategies.

Cloud computing offers tremendous possibilities for global businesses, but to capitalize on these opportunities, IT professionals need to have a familiarity with data-privacy-compliance issues.

I. AN OVERVIEW OF CLOUD COMPUTING

Cloud computing has enabled many businesses to escape the substantial task of creating a computing infrastructure. No longer are businesses tethered to the limitations of brick and mortar as they've gained the nimble flexibility to redeploy employees and other business assets almost on a moment's notice. Gone are the days when the only option for businesses was on-premises computing, requiring a business to purchase, install and maintain its own computer hardware and software infrastructure.

However, the 'cloud' often means different things to different people, especially non-technical staffers. The specifics of cloud computing – especially its deployment models – are important when analyzing its legal and regulatory impact.

DEFINING CLOUD COMPUTING

As IT professionals know, cloud computing – and the advantages stemming from it – involves more than simply storing data on remote servers, a critical point when analyzing the legal and regulatory issues of the cloud.

NIST DEFINITION

When the US government's National Institute of Standards and Technology (NIST) set out to define cloud computing, it ended up taking years of work, input from government and industry, and 16 drafts before it published its final version in October 2011.

NIST defined cloud computing as:

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

NIST noted that its model included five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service), three service models (SaaS, PaaS and IaaS), and four deployment models (private cloud, community cloud, public cloud and hybrid cloud). These deployment models are critical to analyzing data-privacy-compliance issues.

DEPLOYMENT MODELS

PUBLIC CLOUD

The NIST definition of a public cloud is a cloud infrastructure provisioned for use by the general public that may be owned, managed and operated by business, academic or government organizations – or some combination – existing on the premises of a cloud provider. As we look at this definition in 2015, it's important to note that 'general public' doesn't necessarily mean 'consumer.' General public in the context of public cloud computing means that tenants of the public cloud provider – often businesses rather than individuals – share the public cloud infrastructure. For instance, a public cloud provider's datacenter may host the data of various unrelated businesses, such as medical offices, real estate companies and law firms, with their only connection being that they share a cloud provider. Citing cost savings, scalability and flexibility as reasons for their choice, many businesses use public clouds as the method of deployment.

PRIVATE CLOUD

The private cloud is a cloud infrastructure provisioned for exclusive use by a single organization that is owned, managed and operated by the organization, a third party or combination, and exists on- or off-premises. Private cloud is an increasingly popular choice for organizations in heavily regulated industries, those desiring managed services, and other organizations most affected by the legal and regulatory issues discussed below.

HYBRID CLOUD

As the name implies, the hybrid cloud is an integrated approach that may combine the use of public and private cloud infrastructures. However, it's important to note that hybrid clouds often involve more than merely different deployment methods. For instance, the hybrid cloud may be a cloud implementation that integrates multiple cloud applications, on-premises applications or both. The key feature is that hybrid clouds allow organizations to have unique, distinct infrastructures bound together by standard or proprietary technology enabling data and application portability – often with managed services – interoperating to deliver seamless business functions.

CLOUD COMPUTING TRENDS

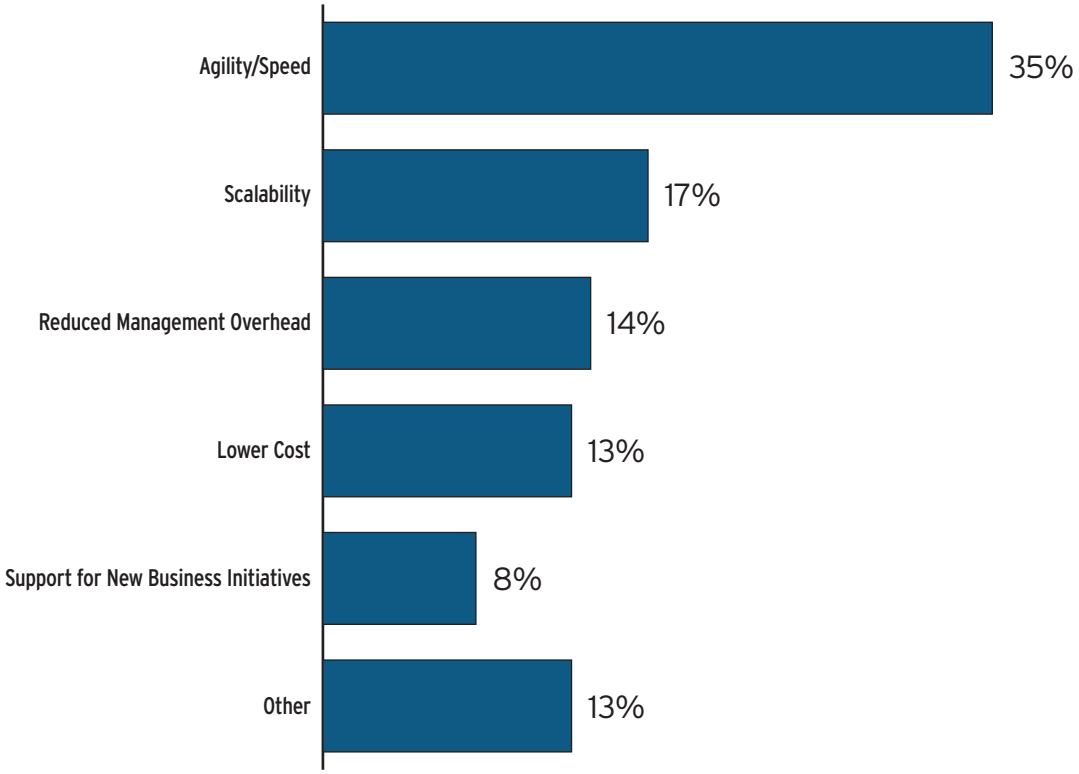
THE GROWTH OF CLOUD COMPUTING

As noted above, cloud computing brings significant advantages to businesses. Recent 451 Research data indicates that cost savings remains the most-often cited business advantage of cloud computing, but other important advantages are shortening the time to market, decreasing what businesses must manage internally and creating new sources of revenue.

PRIMARY BENEFIT OF USING CLOUD

Source: 451 Research

Overall, what is the primary business benfit of cloud computing to your organization today?



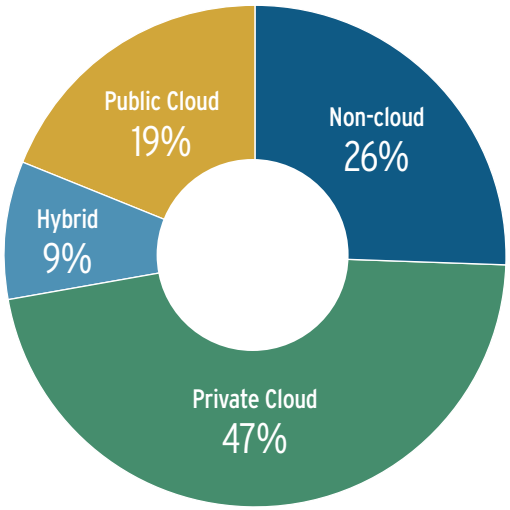
These cloud computing advantages are driving businesses to move to the cloud. In a January 2015 survey by 451 Research, 74% of respondents said the cloud would be their primary deployment method for workloads over the next two years. The largest percentage said they plan to use private cloud deployment, followed by public cloud and then hybrid cloud.

In a survey by 451 Research, 74% of respondents said the cloud would be their primary deployment method for workloads over the next two years – with the majority planning to use private cloud, followed by public and then hybrid.

WORKLOAD DEPLOYMENT BY CLOUD TYPE - NEXT TWO YEARS

Source: 451 Research

Over the next two years, what will your primary deployment method most likely be for each of the follow workloads?



GEOGRAPHICAL EXPANSION OF CLOUD COMPUTING

North America has been the traditional center of cloud computing, but data from 451 Research indicates that other parts of the world are gaining ground. Datacenter activity is a key indicator of cloud computing growth, and North America remains the home of the most datacenters in the world. However, the Asia-Pacific region has surpassed Europe, and it now houses the second-largest number of datacenters in the world, followed by Europe, the Middle East and Africa, and Latin America. In addition, 451 Research predicts that in 2016, the Asian-Pacific region – driven primarily by growth in China – will overtake North America as housing the most datacenters.

The European cloud market is becoming more localized due in large part to Europe's strong data-privacy protections discussed in this report. Meanwhile, the cloud market in Asia is growing rapidly, and now includes about 50 active cloud infrastructure service providers. The total IaaS market in Asia-Pacific stood at $1.27bn for 2014, with the top 10 IaaS vendors collectively generating more than $280m in revenue. The cloud computing market in the Asia-Pacific region, which comprises IaaS, PaaS and infrastructure software as a service, is expected to grow nearly 3.5 times by 2019, from $1.8bn in revenue in 2014 to more than $6.4bn, with a CAGR of 28% through 2019.

The European cloud market is becoming more localized due in large part to Europe's strong data-privacy protections discussed in this report. Meanwhile, the cloud market in Asia is growing rapidly, and now includes about 50 active cloud infrastructure service providers.

II. CURRENT ISSUES IN DATA PRIVACY CLOUD COMPLIANCE

ISSUE ONE: THE MICROSOFT DUBLIN WARRANT CONTROVERSY

At first glance, many IT professionals might think that search warrants related to alleged drug trafficking would have little effect on their businesses, and certainly not on their IT systems. Sure, there's a chance an employee might run afoul of drug laws, but could a drug case affect entire IT infrastructures around the world, as well as how data is transferred in the future? The answer is that it's entirely possible with a case involving New York federal prosecutors, Microsoft, email accounts and servers in Ireland.

BACKGROUND ON THE ISSUE

The case began in December 2013 when a US federal magistrate judge issued a criminal search warrant to US government prosecutors in a narcotics trafficking case. The government sought the warrant to search and seize email content data and other information stored on servers at a Microsoft datacenter in Dublin. Microsoft asked the court to invalidate the search warrant, arguing that US courts were not authorized to issue warrants beyond the borders of the US.

The legal issues in the case are complex and involve technical nuances of US laws, including the *Stored Communications Act* (SCA), part of the *Electronic Communications Privacy Act of 1986* (ECPA), and the *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, known commonly as the USA PATRIOT Act.

In a nutshell, a primary legal argument between Microsoft and US prosecutors pits Microsoft's argument that the US government has no authority to issue a search warrant in Ireland against the prosecutors' argument that, under current US law, it matters not where the data is stored, but who controls the data – in this case, Microsoft, a company based in the US and subject to a US search warrant. So far, the US courts have sided with prosecutors, but Microsoft is appealing the decisions to a US federal appellate court.

WHY IT MATTERS AND GUIDANCE FOR THE IT PROFESSIONAL

This issue matters because if the US appellate courts uphold the case, which may even go to the US Supreme Court, US prosecutors may try to execute search warrants around the world. Such US data-gathering attempts would, in all likelihood, trigger a backlash from many governments and global businesses. Aware of the danger such warrants could pose to the US tech industry, various US companies and organizations that are not parties to the case – including AOL, Apple, AT&T, eBay, Hewlett-Packard, the National Association of Manufacturers, the National Newspaper Association and the US Chamber of Commerce – have filed friend-of-the-court briefs supporting Microsoft's position.

IT professionals should be aware of the national origin and legal status of the cloud vendors they use because origin and legal status could subject them to claims from national governments associated with the vendors. They should also be aware that such claims are not limited to the US government. As we'll discuss later in this report, many national governments claim the right to search data in criminal and national security investigations. The importance of the Microsoft Dublin warrant controversy is that it shows that such claims don't stop at national borders, and we encourage IT professionals to follow this case.

IT professionals should be aware of the national origin and legal status of the cloud vendors they use because origin and legal status could subject them to claims from national governments associated with the vendors.

ISSUE TWO: INTERNATIONAL E-DISCOVERY AND E-DISCLOSURE

Perhaps nowhere is the dilemma of the technologically efficient delivery of data versus the need to protect sensitive information more acute than in cross-border data transfers. As international business has become more common, so has international litigation, making discovery in legal proceedings a major source of international data transfers. Cloud computing has made these data transfers easier from a technological standpoint, but such quick and easy transfers can create compliance challenges.

BACKGROUND ON THE ISSUE

Known as e-discovery in the US and e-disclosure in the UK, this process of litigation evidence-gathering results in large volumes of data being transferred internationally. E-discovery in the US is especially significant because the US system has a legal tradition of giving litigants and lawyers extensive access to evidence, which is at odds with traditions in other nations – perhaps most notably, the member states of the European Union.

Even the UK, the birthplace of discovery, does not have the extensive e-discovery practices found in the US. Most nations of Continental Europe are even more unlike the US on the issue of e-discovery, largely due to their civil law tradition in which evidence is collected by judges in an inquisitorial system – unlike the juries receiving evidence in common-law traditions of the UK and the nations that have adopted its English common-law system, such as Australia, Canada, most of India, Ireland, the Chinese possession of Hong Kong, Singapore and most of the US.

In addition, specific provisions of the US Federal Rules of Civil Procedure give litigants in US courts a great deal of latitude in demanding evidence for electronic discovery – especially after e-discovery amendments to the rules in 2006, which popularized the legal technology term 'electronically stored information.' Indeed, the differences between US e-discovery and evidence procedures in the rest of the world are something businesses that employ cloud computing should monitor.

European nations have taken steps to prevent US demands to violate their evidence-based sovereignty. They have gone so far as to enact so-called blocking statutes to provide penalties for transferring documents for use in foreign proceedings unless the transfer complies with the provisions of the *Convention on the Taking of Evidence Abroad in Civil and Commercial Matters*, known commonly as The Hague Evidence Convention.

Perhaps the most well-known blocking statute is the French blocking statute of 1980, Law 80-538. This statute provides criminal penalties, including imprisonment, for parties transferring documents or information relating to commercial, economic, financial, industrial or technical matters outside France without complying with the provisions of The Hague Evidence Convention.

WHY IT MATTERS AND GUIDANCE FOR THE IT PROFESSIONAL

The IT professional should proceed with caution when receiving a legal demand for cloud data. It goes without saying that IT staffs should consult with counsel before releasing corporate data. International e-discovery is a major compliance issue because IT professionals may receive a demand for data that is perfectly legal in the US but that is contrary to the laws of other nations, most notably the blocking statutes discussed above and the international data-privacy laws discussed below. Thus, perhaps the most important compliance guidance for the IT professional when it comes to international e-discovery and e-disclosure is to be aware of these conflicting laws. It's not necessary for IT professionals to know every nuance of international data-transfer laws – just be aware they exist. It may seem as though compliance best practices would call for compliance with legal demands for cloud data. Paradoxically, proper compliance procedure may be to refuse to comply with these legal e-discovery data demands – after consulting with counsel, of course.

IT professionals may receive a demand for data that is perfectly legal in the US but that is contrary to the laws of other nations

ISSUE THREE: THE US-EU SAFE HARBOR FRAMEWORK

Under the 1995 EU Data Protection Directive, known formally as *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, which became effective in 1998, data can be transferred outside the EU only to nations that meet adequate data-privacy requirements under EU law. The US does not meet such standards, but data transfers can be made under an agreement known as the US-EU Safe Harbor Framework.

BACKGROUND ON THE ISSUE

There are actually two Safe Harbor Framework agreements: one between the US and the EU and another between the US and Switzerland. They are administered on the US side by the US Department of Commerce. Approved in 2000, the US-EU Safe Harbor Framework allows data transfers by binding the 28 member states to the EU Commission's finding of data-protection 'adequacy' based on a company's certification under the Safe Harbor Framework. In essence, individual companies obtain EU certification to transfer data even though the US itself does not meet European data-protection requirements. About 3,200 companies have obtained Safe Harbor certification, and under the current system, compliance is based on self-certification, meaning the companies themselves certify that they're in compliance.

The Safe Harbor Framework is in trouble, however. In a 2014 European Parliament resolution that passed 544-78, the Parliament called for suspension of the Safe Harbor Framework. In addition, in March 2015, the EU Court of Justice heard arguments in *Schrems v. Data Protection Commissioner*, a case from Ireland challenging the Safe Harbor Framework. In referring to the case, the High Court of Ireland said, "There is, perhaps, much to be said for the argument that the Safe Harbor regime has been overtaken by events. The Snowden revelations may be thought to have exposed gaping holes in the contemporary US data protection practice."

Negotiations between the European Union and the US on the future of the Safe Harbor Framework continue, and the EU Court of Justice decision should come later this year.

WHY IT MATTERS AND GUIDANCE FOR THE IT PROFESSIONAL

IT professionals involved in cloud data transfers between the US and Europe should be aware that the Safe Harbor Framework is at risk and that, without Safe Harbor, their ability to transfer data will be in jeopardy. Organizations thinking about cloud services should also be aware that, even if the Safe Harbor Framework does survive, the self-certification system might not, meaning that US vendors transferring data could have new compliance responsibilities overseen by government regulators.

IT professionals involved in cloud data transfers between the US and Europe should be aware that the Safe Harbor Framework is at risk and that, without Safe Harbor, their ability to transfer data will be in jeopardy.

ISSUE FOUR: THE EU GENERAL DATA PROTECTION REGULATION

The European Union is considering a General Data Protection Regulation (GDPR), which would replace the current EU Data Protection Directive. When considering the move from the EU Directive to the proposed General Data Protection Regulation, the distinction between 'directives' and 'regulations' under EU law is significant.

BACKGROUND ON THE ISSUE

An EU regulation is a binding legislative act that must be applied in its entirety throughout the 28 member states in the EU. An EU directive, on the other hand, is a legislative act establishing EU policies that are implemented through laws passed by the member states themselves. For instance, the 1995 EU Data Protection Directive mandated that EU member states pass corresponding data laws by October 1998, but the member states still had discretion on their individual laws because the data-protection legislation was a directive, not a regulation. The implementation of the GDPR, of course, would change that.

Among the issues under consideration with the GDPR are one-stop shop for data-protection authorities, non-EU data transfers, non-EU legal process, consent, fines, corporate data protection officers, data breach notification, and the right to be forgotten/right to erasure. The EU Court of Justice jumped the gun on the GDPR in May with its 'right to be forgotten' (the concept that individuals have the right to ask for personal information to be removed from the Internet) decision in *Google Spain SL v Agencia Española de Protección de Datos,* in which the court held that a right to be forgotten existed under the 1995 Directive with certain limitations.

WHY IT MATTERS AND GUIDANCE FOR THE IT PROFESSIONAL

The GDPR is a critical data-privacy-compliance issue for any organization involved in cloud data transfers involving the EU member states (Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK) and the additional three nations (Iceland, Liechtenstein and Norway) that – along with the 28 EU member states – make up the European Economic Area (EEA). Although the idea behind the GDPR is to harmonize the laws of the member states to make data protection – and thus commerce – easier throughout Europe, organizations need to be aware of how it will affect their cloud strategies. Although the European Commission and the European Parliament have approved the GDPR, it must also be approved by the Council of the EU (not to be confused with the Council of Europe – a completely separate organization) for it to go into effect.

Compliance guidance for the IT professional includes following the outcome of the 'one stop shop' provisions, the future of working with data-protection authorities, as well as the consent provisions for the transfer of personal data. Fines are also an important compliance consideration. Initial proposals included fines up to €1m or 2% of an offending company's annual revenue. That proposal has increased to €100m or 5% of a company's annual revenue.

Compliance guidance for the IT professional includes following the outcome of the 'one stop shop' provisions, the future of working with data-protection authorities, as well as the consent provisions for the transfer of personal data.

ISSUE FIVE: EXPANSION OF DATA PRIVACY LAWS AROUND THE WORLD

Although data transfers between North America and Europe often capture a great deal of the attention in discussions of data-privacy compliance, the expansion of data-privacy laws around the world is a significant issue.

BACKGROUND ON THE ISSUE

Comprehensive data-privacy laws are nothing new in many nations around the world, but laws such as the USA PATRIOT Act and developments such as the NSA-Snowden controversy have helped pass new legislation with data-privacy provisions, such as Brazil's Marco Civil da Internet. At the same time, although many laws have strengthened data-privacy protections, other laws under consideration to address perceived terrorist threats have been criticized as potential threats to data privacy.

The chart below summarizes data-privacy developments around the world:

NATION	LAW/REGULATION
Australia	Australian Privacy Principles (APP)
Brazil	Marco Civil da Internet ('Internet Constitution')
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
Canada	Provincial Data Privacy Laws
China	Law on Guarding State Secrets
China-Hong Kong	Personal Data Privacy Ordinance
Germany	Bundesdatenschutzgesetz (Federal Data Protection Act)
Japan	Personal Information Protection Act (PIPA)
Russia	Localization Act
Singapore	Personal Data Protection Act (PDPA) and Regulations
USA	HIPAA – Health Information Portability & Accountability Act
USA	FERPA- Federal Educational Rights & Privacy Act
USA	USA PATRIOT Act
USA	ECPA – Electronic Communications Privacy Act

WHY IT MATTERS AND GUIDANCE FOR THE IT PROFESSIONAL

The expansion of data-privacy laws around the world is a significant issue because it may present some challenges and require due diligence when preparing for cloud computing. Legal developments such as Russia's Localization Act run counter to the technological promise of efficient cloud computing. In essence, law (and politics) can become as important as technology (and business considerations) in the development of cloud computing. Compliance guidance for the IT professional includes advice that may seem simple: know where your data is. Organizations should question their cloud providers about where data is housed. In addition, organizations should make international data-privacy laws a primary consideration in the selection of cloud providers and datacenter locations.

III. CONCLUSION

Whether due to the pending EU General Data Protection Regulation, increased regulatory enforcement in the US or the expansion of data-privacy laws around the world, the most important compliance guidance for the IT professional hoping to harness the power of cloud computing may be:

1. Know where your data is.
2. Have at least a basic familiarity with international data-privacy laws and regulations where your data is housed.
3. Secure your data.

Data breaches aren't going to stop anytime soon. Using the US as an example, there are 47 state data-breach-notification laws, and the US Federal Trade Commission is stepping up data-breach enforcement. In addition, the pending EU GDPR has stringent data-breach provisions, and data-breach laws exist in jurisdictions around the globe. IT professionals should also remember that many times, a breach has nothing to do with hackers; inadvertent breaches are an important part of data security. Securing data is critical, and – bringing things full circle – cloud computing itself can be an efficient way to secure digital data.

Cloud computing programs should include service-level agreements that have provisions for data-breach protection and data location along with provisions for retrieval of data. In essence, IT professionals should ensure that data is secured, its location is known at all times, and that it can be retrieved easily.

Many of the legal and regulatory challenges facing cloud computing can apply to other forms of data deployment. For instance, the challenges of cross-border data transfer existed long before cloud computing. The cloud just makes these transfers easier and quicker, which can increase the legal and regulatory risk. The bottom line is that each of the five issues addressed in this report may, with due diligence and the right cloud provider, actually help companies meet and realize the promise and benefits of cloud computing.