Cloud Computing: Is Regulation Good For You?

By Taiye Lambo

July 2012

Within the past month, authorities across Europe and the United States have taken a series of steps that mark the first move towards regulation of cloud computing. The European Commission's panel on privacy, known as the Article 29 Working Party, released a series of guidelines related to their opinion on cloud computing in the European Economic Area (EEA). This is the first time that a working party within the European Union (E.U.) has explicitly endorsed cloud computing; previous approaches to cloud computing have been cautious and tepid at best. The working party's move helps highlight the need for cloud service providers and their customers to ensure that data stored in the cloud is properly secured. There is a potential for this to inform and influence the decisions being made by regulators in the 27 E.U. member countries. Shortly thereafter, the USA's Federal Financial Institutions Examination Council, or FFIEC, followed suit with their own guidance for cloud computing in the financial services industry. This move, while not regulation per se, will attract attention and certainly give the cloud increased attention from U.S. banks. History shows that guidelines like those released by the Article 29 Working Party and FFIEC are often precursors to regulations. If this is, in fact, the case, what would cloud computing regulation mean for you?

Here are some of the pros and cons of the recent moves towards cloud computing regulation and their potential down-the-road implications.

Pros of Cloud Computing Regulation:

1. *Increased Adoption of Cloud Computing Services*

   The Article 29 Working Party guidelines will likely spur adoption of cloud computing services in the E.U. in a significant way. The research firm Gartner estimates that the E.U. is at least two years behind the United States in the adoption of cloud computing. Most of the pioneering cloud computing work by firms like Google Apps, Salesforce.com, and others has been done in the United States. One of the reasons why the E.U. has lagged behind has been security and privacy concerns. The guidelines have the potential to stimulate the European cloud computing market from both the provider and consumer standpoint. Guidance and leadership from European authorities on issues related to cloud computing may

help allay some of the security and privacy fears and help the E.U. catch up in terms of cloud computing adoption and strategy.

2. *Increased Attention to Security and Privacy Issues*
   Universally accepted cloud computing security standards have yet to emerge. Organizations use a variety of certifications and until the ISO/IEC 27017 cloud security standards is released, none of the existing security certifications are specifically designed for the cloud. There is a great deal of extremely sensitive information stored on the cloud and much of it is vulnerable to unauthorized access. Unless these issues are addressed quickly in a uniform and consistent manner, there is a very serious chance of an impending cloud disaster. The right regulators stepping in at the right time to provide guidance could potentially mitigate some of these issues. Such actions taken along with the promise of further regulatory action can prompt cloud service providers to step up their security and privacy initiatives. Fear of fines and even potentially jail-time can force providers to implement holistic risk-based security and privacy programs that involve their full range of stakeholders including vendors and consumers. Industry standards are optional, but regulatory requirements are mandatory; knowing this, many providers will pay increased attention to security and privacy issues.

Cons of Cloud Computing Regulation:

1. *Increased Complexity and Costs of Cloud Services*
   Any industry with a strict regulatory environment experiences financial and opportunity costs of doing business. From legal costs, to fines, to compliance efforts, to foregone business, regulations can be a barrier to business. There is also the danger that these E.U. guidelines and future regulations may spur individual member countries to create their own individual regulatory frameworks for cloud computing security and privacy. Countries like Greece and Spain that are seeking ways to immediately cut costs are especially likely to look into adopting cloud computing, which could include local cloud computing regulations. Once this happens, other EU member states could follow suit, which could possibly create a myriad of different cloud computing regulatory frameworks within the E.U. In this case, a provider seeking to offer their cloud services across Europe would face an overwhelming obstacle in demonstrating compliance with potentially conflicting regulatory requirements. Additionally, cloud consumers who do not fully understand the nature of the guidelines may view the cloud as being more dangerous because these guidelines reveal major threats that would otherwise go unnoticed by the average cloud consumer.

2. *Increased Superficiality of Security and Privacy Initiatives*

   One of the major downsides of regulations in general is that it shifts the nature of individual action. Organizations that currently implement security and privacy initiatives do so of their own volition and are driven by a strategic and principled application of best practices in accordance with their strategic business needs. However, in a more regulated cloud computing environment, these current actions will likely need anything from further documentation to major revisions to meet regulatory requirements. Regulations often result in more of a compliance driven approach to security and privacy, what we call the "checkbox mentality." Regulators may develop a series of requirements and providers may meet the letter of the law, but not its spirit. In my 15 years of information security management, I've learned that *compliance does not equal security*. Organizations must take a holistic, risk-based approach to cloud computing security and privacy; if not, they will always be one (if not ten) steps behind the bad guys.

In summary, we recognize a great need for greater cloud computing security and privacy across the board and the guidelines taken especially by the E.U.'s Article 29 Working Party and USA's FFIEC are a welcome first step. However, there are potential negatives to regulations that must be avoided by educating the consumer on risks associated with the cloud and ensuring that the checkbox mentality does not prevail with cloud service providers. If these concerns can be addressed, this month's countdown to the regulation of cloud computing could be a step in the right direction.

About the Author: Taiye Lambo is a seasoned entrepreneur with Global Information Security and Governance, Risk Management and Compliance expertise with a focus on Cloud Computing. He is the Founder of USA based CloudeAssurance, Inc., eFortresses, Inc., the Holistic Information Security Practitioner Institute (HISPI) and the UK Chapter of the Honeynet Project and can be contacted via E-mail (tlambo@eFortresses.com), LinkedIn (http://www.linkedin.com/in/taiyelambo) or Website (www.CloudeAssurance.com).