# Chapter 1
# Cloud State Surveillance:
## Dark Octopus Tentacle Clouds from the Atlantic

**Sylvia Kierkegaard**
*International Association of IT Lawyers, Denmark*

## ABSTRACT

*Concerns about government snooping in the wake of revelations by whistle blower Edward Snowden have deterred enterprises and IT professionals from keeping sensitive data in the clouds. Moving towards cloud-based computing has emerged and has gained acceptance as a solution to the tasks related to the processing of information. However, cloud computing carries serious risks to business information. The questions around risk and compliance are still largely unknown and need to be ironed out. Cloud computing opens numerous legal, privacy, and security implications, such as copyright, data loss, destruction of data, identity theft, third-party contractual limitations, e-discovery, risk/insurance allocation, and jurisdictional issues. This chapter discusses the associated legal risks inherent in cloud computing, in particular the international data transfer between EU and non-EU states.*

## 1. INTRODUCTION

Information is the heart and soul of many businesses. The information that companies generate and share are generating a wealth of benefits. E-mail, social media, mobile phones, drop boxes, increased internet devices and broadband connections have enabled businesses and consumers to exchange high data volumes and files everywhere and over vast networks with high speed communication.

Information is now available and shared to an extent almost unimaginable 10 years ago due to the increasing digitization and modern technology. At the same, it has caused organizations to struggle with the high volumes and diversities of information and seek solutions to manage the information and to reduce cost through effective information governance.

Information Governance (Info Governance) is the specification of decision rights and an accountability framework to encourage desirable

DOI: 10.4018/978-1-4666-7381-6.ch001

behaviour in the valuation, creation, storage, usage, archiving and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information to enable an organization to achieve its goals. (Logan, 2009) These include the management of information securely, efficiently and effectively—what information is retained, where and for how long, and how it is retained (e.g., protected, replicated and secured), who has access to it and how the polices are enforced. They encompass not only suitable policies, accountability, and procedures but also the technology to create a solid governance framework. Unmanaged and inconsistently managed information increases risk and cost.

Information technology officers are looking for technologies that will help them focus more on the benefits to the organization, which can bring institutional agility, flexibility and cost saving. Moving towards cloud-based computing has emerged and gained is acceptance as a solution to the tasks related to the processing of information. The IT industry has witnessed a rapid adoption of the public cloud and many have migrated enterprise applications to the cloud. Cloud promises a single portal view to better manage email, archiving, and records retention (etc). Since web 2.0, "cloud computing" has been the buzz word in the IT industry. Cloud advocates argue that implementing any form of IT or information governance is far easier and far more effective in a fully-virtualized private cloud model than in the traditional, physical IT world.

The promise of a utility-based IT service delivery model is well understood and highly desirable. The greatest gain for business is that cloud services can create advantage cutting out hardware costs and reducing their costs per unit as demand increases while for enterprise customers, it enables information to be accessible from any device that is connected to the Internet.

However while cloud computing certainly brings efficiencies, it is still immature and carries serious risks to business information. Many companies are still hesitant to move their core business applications into the cloud until cloud providers address several main concerns, including security, control, customization, and complexity. The questions around risk and compliance are still largely unknown and need to be ironed out. As the adoption of cloud computing continues to grow across the world, security, privacy and regulation of data in the cloud is becoming more prominent and relevant.

A survey, which was carried out at RSA Conference 2014 in San Francisco, looked at the attitudes of nearly 280 IT security professionals towards cloud security. A third of IT security professionals do not keep corporate data in the cloud because of fears of government snooping. In the same survey conducted in 2012, 48% of respondents were discouraged from using the cloud because of fear of government snooping, while 86% preferred to keep more sensitive data on their own premises (Ahford, 1014).

The European Union is addressing the challenges concerning the threat to information security specific to cloud computing through several measures. While businesses and governments wax lyrical about the benefits of cloud computing, EU regulators have been more wary, as further take-up of cloud systems would mean a large swathe of public and commercial data would migrate to servers possibly located outside national borders or even on other continents.

Despite the EU's best efforts, laws to protect and store data are outdated and cannot cope with the legal problems presented by cloud computing, such as determining who owns data which is no longer handled in situ. This article will provide an overview of cloud computing and discuss the current and legal risks for businesses using cloud computing, especially state surveillance on private citizens.