Media in the Cloud: new world shaped between technology and law.

Alicja Gniewek
Master en Droit Européen LL.M

***

PhD Candidate
Interdisciplinary Centre for Security Reliability and Trust
University of Luxembourg

Abstract

Cloud Computing (CC), a new major trend in ICT, is a concept which could reshape the virtual media landscapes. New features of CC such as dynamic data distribution and resource sharing allow for outsourcing and then processing, storing and sharing massive amounts of data via networks of data centers. CC provides efficient services accessible via simple interfaces without having additional costs like in-house datacenters and IT personnel. These features of Cloud Computing could and have encouraged many businesses to migrate to the Cloud.

This paper aims to analyze and interpret current EU legal requirements dealing with data protection in the context of technical features of Cloud Computing in order to provide a coherent view of the development of media business in the Cloud as well as its constraints.

Distributed computing has so far introduced new kinds of media communications that were widely adopted, e.g. blogging, social networking sites and electronic newspapers. Some of them like Facebook, Twitter and services provided by Google are based on Cloud Computing technology. Data, that contain often personal details are being migrated from users' computers to the Cloud, processed and stored by Cloud Providers. Security of these data remains open question due to often unclear privacy policies.

This paper names the legal consequences and problems that arise from the usage of Cloud Computing in virtual media. Bearing in mind the core feature of the Cloud that is outsourcing of data in a most cost-effective way, fundamental issues that arise are the legal consequences of the location of data centers and data protection law applicable to data stored there. Access to data, interoperability and retention policy are the next problems that need to be addressed due to, *inter alia* their direct and daily consequences for each individual user. Finally anonymization and re-use of data in the Cloud constitute the legal concerns.

Paper aims to demonstrate the technical and business advantages of Cloud in the context of data protection risks. Foreseen outcome of this study is an outline of possible direction of changes in New Media caused by Cloud adoption. Two case-studies are examined – Facebook privacy policy analysis as well as Google privacy policy study. The latter was altered on 1st of

March 2012. It has replaced service-specific privacy policies and introduced one, relatively short privacy policy. This move caused a huge outcry on many continents – despite the fact of information campaign carried out by Google and possibility of one-way opt-out, it created great uncertainty among users that was fueled by the press. Legal authorities concerned with data protection have also taken part in the discussion.

The most interesting, from media perspective, element of the Google's change is the possibility of combining user's data across-services, e.g. search engine results, e-mails content, blogging and personal details given by the user while creating Google Account. On the one hand it can create a new value in media world – as the information obtained by user could be to the greater extent customized according to their preferences. On the other hand it could harm the freedom of speech, as by the means of profound profiling each user could be tracked (e.g. their blog entries and their forum postings could be linked to their personal details and no longer be anonymous). It induces such data protection questions as, *inter alia*, access to this data (government?) as well as data retention (deletion from the active servers as well as from the backup servers). As a consequence – profound profiling of individuals may induce massive abuses, among others: hacking, identity theft, "fishing expeditions" (police/government requests certain data of people that match certain profile) as well as crossing currently unknown privacy barriers.

Facebook, an example of social networking site, has recently introduced two huge changes that are adopted by default, namely: Timeline and facial recognition technology. These changes, e.g. combining and sharing user's data by Facebook without proper information given to users could cause major privacy concerns and risks for users, e.g. hacking "craft attacks". As recent studies show user's knowledge about privacy and willingness to manage their profile has gradually increased. Balancing these two factors (Facebook and user's pursuits) is an unanswered problem that seems to be crucial for the development of such kind of social networking sites.

All the above mentioned issues are tackled in this paper taking in mind relevant EU data protection rules, namely European Data Protection Directive (Directive 95/46/EC) as well as legislative proposals adopted by the European Commission within the scope of a reform of the EU legal framework on the protection of personal data.