executiveupdate

Legal and Public Policy Aspects of Cloud Computing

Cloud computing seems a hype, but evolved as a key delivery model for digital technology and information provision for both the private and public sectors. One that will not blow over. Addressing its legal and public policy aspects is a condition sine qua non for successful deployment, whether done by the in-house IT department or outsourced to cloud server providers. The law plays a double role in respect to cloud computing. It functions as a legal framework set by mandatory laws and regulations, *and* as a contractual instrument to manage the 'new style' technology and information provisioning in an effective and sustainable way, based on the strategic objectives of any organization — large and small.

Victor A. de Pous, May 15, 2012 — for The 4th China Cloud Computing Conference, May 23-25, 2012, Beijing (www.ciecloud.org/2012), Chinese Institute of Electronics

□ Headlines

- Place-and time-independent acting by people (in private life, for work, business and government) and increasingly between things (THE INTERNET OF THINGS) compose the consolidated mega trend in our society, enabled, facilitated and innovated by cloud computing.
- Cloud computing is not a (new) technology, but relates to a method of IT delivery as an on-demand and automated-scalable service over the Internet, based on supply chain automation in data centers — evolutionary caused by virtualization, web-based data processing and the generic and accessible availability of broadband Internet.
- Cloud computing also holds the promise of scalable and secure services for greater efficiency and flexibility, at lower cost. This also applies to government organizations.
- Doing nothing is no option. Cloud computing is a *key and unavoidable IT delivery model*. Public sector organizations, enterprises, and even small and medium-size companies simply cannot avoid making policies for cloud services. In this respect the law plays a double role. It functions as a legal framework created and compiled by diverse mandatory laws and regulations, *and* as a contractual instrument to manage this new style technology and information provisioning in an effective and sustainable way, based on the strategic goals of the individual organization.

□ Cloud computing framed

What constitutes cloud computing? A computer scientist draws computers and software services and connects them to the Internet. Thus 'the cloud' was born, as a metaphor. Search engines Lycos and Yahoo (1994) and the e-mail service Hotmail (1996) were examples avant la lettre, but the first airline reservation system around 1960 already used a cloud model. Exemplary today, Amazon Web Services, Salesforce, Google Docs and Microsoft Office packages Office365 and the immensely popular social networks Facebook and YouTube - not to mention the literally countless apps for smart phones, tablets and more.

Cloud computing takes place largely invisible, but it shows itself to end-users as web-based software and information that is stored on servers in data centers *elsewhere* and no longer on their computers or information systems of the organization they work for. The actual processing is done *virtualized* – the computer programs and information are disconnected from the physical hardware and infrastructure. Consequently, the nature of data (processing) changes in non-permanent and dynamic, and becomes almost 'liquid'.

Cloud computing developed and keeps developing in an *evolutionary* way. Technologically speaking, the turning point lies behind us, because essential information technologies, including virtualization and broadband Internet, are now widely available and accessible. Cloud computing may be a service provided by the *internal* IT department, but cloud computing will more likely involve an outsourcing relationship. At the CloudGov 2012 conference, the Department of Homeland Security of the United States asked rhetorically 'Are we in the data center business or do we need IT functions?'[1]

According to the internationally broad-accepted definition, the National Institute of Standards and Technology (NIST) 'describes how cloud computing is 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.'[2] The cloud matrix comprises PUBLIC (open and standardized), PRIVATE (closed and any desired length), COMMUNITY (targeting a particular community) and HYBRID (public/private) application models and distinct in the service model (SaaS) software, platforms (PaaS) and infrastructure (IaaS).

□ Major legal reference points

That cloud computing is both technologically and commercially something fundamentally different, does not mean in advance that the legal aspects differ. Nevertheless, anyone who keeps NIST's definition in mind, is probably not surprised that its legal framework indeed deviates from the more conventional client/server model for electronic data processing. *Cloud computing experiences difficulties with existing legal rules, which are a) not only by tradition defined*

[1] Washington, DC, February 16, 2012.

[2] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

geographically, but also b) established during a time-period when corporate and government information had a static character. We could literally pinpoint where the data was located.

Also enclosed in the cloud delivery model are all kinds of technical, organizational and social aspects, together with the consequence that *horizontal* (applicable to all organizations), *vertical* (additional for regulated industries) and *specific IT-related legal rules* apply to cloud computing. That leads to legal concurrence. Furthermore, we note various developments, such as new insights, best practices, and initiatives for the certification of cloud services. Next to those, new privacy regulation for personal data is on its way for the 27 European Union member states, which strengthens and harmonizes the existing 1995 legislation in this domain.[3]

Yet we must not make the legal aspects of cloud computing more difficult than what they are, *and* always evaluate the characteristics of a cloud service in a particular case. A number of marks provides guidance and direction for legal analysis, policy development and drafting agreements. Take for example the case that a governmental department or municipality wants to open its data for reasons of transparency or re-use by entrepreneurs. Because of its practical characteristics, a PUBLIC cloud service comes into view immediately: web-based with flexible scalability, open, and for anyone remotely accessible via Internet. All self-provision. Concerns about information security and adverse effects of the reach of foreign jurisdictions no longer exist, because the processed information is not confidential and does not affect personal information.

Reference point #1 Self-provisioning or outsourcing?

A central legal theme for cloud computing relates to the question whether or not an outsourcing relationship exists. When any organization outsources an IT service to an external CLOUD SERVICE PROVIDER, in principle it loses control over the information processing process, unless other contractual arrangements are made. Further, there is a strong situation of dependency towards both supplier and the used technology, partly because, in particular, software *and* information are in the hands of this supplier (and his suppliers). Outsourcing means at least a shift in technical responsibilities from customer to CLOUD SERVICE PROVIDER, while the customer still keeps its own legal responsibilities, e.g. towards tax authorities.

Reference point #2 Product or service?

Various *factual* aspects of the cloud delivery model have *legal* implications. First of all, cloud computing is not a product but a service and in respect to software as a service (SaaS), the end-user usually receives no physical copy of the computer program he uses remotely. Under European law, the licensee loses his statutory right to error correction, as defined in the European software directive (2009/24/EC). Cloud computing has also effect on licensing models. We note that, due to virtualization, a one-to-one relationship with hardware and operating system no longer exists. *A license agreement must normally allow virtualization*.

[3] [3] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Moreover, producers of original software must deal with the circumstances that in the appropriate case when providing *third-party software*, the license agreement must grant this right to the CLOUD SERVICE PROVIDER.

Reference point #3 Technology or information?

Digital technology concerns the notorious bits and bytes, and brings us eventually back to the ones and zeros. There is, however, a distinction. What do they form: a computer program or data? That question plays a central role seen from a technological perspective, as well as legal framework. Both sharply divide between software code and information in digital format. With this boundary, suppliers and customers of cloud services have to deal. Accordingly, within the European Union, for example, statutory protection rights for software code exist, primarily benefitting the developer (licensor), with the exception of some basic rights for software users (licensees), including the right to make a backup. For (digital) information, an entirely different legal framework is applicable.

Reference point #4 Type of data?

Another important pointer for determining the legal framework for a cloud service is the distinction between *personal data* — relating to for example citizens, consumers, patients, employees — and other information processed by organizations. The nature of the data determines the applicable legal framework, which in turn may influence the choice of a particular IT delivery model.

Reference point #5 Transborder data processing?

Cross-border data processing raises legal questions in relation to the international applicable laws and the competent courts.

□ Ten analyses

1. Cloud computing means diversity. There is not just one cloud. Every type of cloud service includes unique characteristics and related legal aspects, advantages and disadvantages. This diversity requires insight and nuance. Moreover, it is important that both the general pro and con debates, and the discussions in a particular case are conducted on rational grounds. Only than pragmatic policy and individual decision making come within reach.
2. Doing nothing is no option. Even a company or public sector organization that focus solely on cost reduction, do not escape from cloud computing. It goes without saying, however, that organizations must look further than financial reductions. This translates into the circumstance that *strategic goals* should determine the use of information technology. Digital technology plays a key role in numerous change processes. Cloud computing in particular creates organizational (e.g. business agility) and social changes (towards a 'better' society).
3. Although the full transition to cloud services is possible, the practice, at least for public sector organizations will almost certainly show a mixed

delivery environment. The need to process national secrets per se in the cloud, is missing. A mixed portfolio consists of both traditional *and* cloud computing — by both the internal organization *and* third parties.

4. A 2003 European Union policy states that every public sector organization within its 27 member states must offer today the widest possible access to government data for citizens and business (transparent government) and make that data available for reuse (economic development). This so-called 'open data, unless' rule brings a substantial boost for *outsourced* public sector clouds.

5. In particular, cloud services as *a form of outsourcing* raise high expectations. In the words of the European Commission: scalable and secure services for greater efficiency and flexibility, lower costs without large investments. Moreover, we see the advantage of economies of scale and *the economy of skills*. From a legal viewpoint, software as a service (SaaS) means the end of software piracy *at the end-user side*.

6. The benefits for cloud customers do not take away concerns about information security and legal uncertainties. Nevertheless, there are various means available — such as data classification, existing standards and certifications, open data formats, legal frameworks and specific rights (e.g. for interoperability), security arrangements, negotiating terms in cloud contracts — that strengthen the legal position of cloud customers and make risks manageable.

7. Technology standards often intensify the policy debate. The starting point is that the numerous existing IT standards will find their way in the cloud environment. Both the U.S. federal government[4] and the European Commission[5] pursue a pragmatic policy based on RAND: they must be available on (fair,) reasonable and non-discriminatory terms.[6]

8. Although interoperability is a much-debated topic, not every cloud service provider and cloud customer is aware of a legal — even statutory — right under European Union Law. Each licensee of a computer program has the right to decompile the code for unlocking hidden specifications of the program's interfaces, in order to make a connection with other software.

9. Information security is a major concern. So far, however, there is no real technical vacuum or absence of standards as such, because existing standards remain in force for the deployment of cloud computing. NEN-ISO/IEC 27000 is an example.

10. 'Bring your own device' (BYOD) — the fact that directors and employees use their own laptop, tablet and/or smart phone for work — does not raise questions about the hardware, but about software, apps and corporate information *in the cloud*. New work policies are needed.

[4] http://www.whitehouse.gov/omb/circulars_a119/

[5] http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

[6] http://en.wikipedia.org/wiki/Reasonable_and_non-discriminatory_licensing

Legal and Public Policy Aspects of Cloud Computing is written by Victor A. de Pous, an Amsterdam-based corporate lawyer and industry analyst. The author has been working in the domain of the legal and policy aspects of digital technology and the information society since 1983. Victor de Pous is the Legal counsel of International Federation for Information Processing IFIP (http://ifip.org) and the co-founder and member of the board of EuroCloud the Netherlands, the Dutch Chapter of EuroClould (http://www.eurocloudnl.eu).
Julianapark, 16 Anton Constandsestraat, Post Office Box 51005, 1007 EA Amsterdam. Telephone: +31-20-665.57.38, Fax: +31-20-665.58.18, E-mail: depous@planet.nl, Blog: http://depous.blogspot.com/
Fonds: http://technologierecht.blogspot.com/

Leitmotiv

Addressing the legal aspects of digital technology strategically creates economic value, reduces risks and optimizes

History

During its first 50 years computer law referred to a loose collection of diverse legal aspects of electronic processing and

Advancement

A more advanced and structured approach to computer law in the 21st century focuses on legal frameworks for the

Information society

Computer law today must provide solid, well-balanced legal constructions for living, working, and doing business in a sustainable information

assets.	communication of data.	demand-driven availability of robust, secure and interoperable digital products and services.	society, fitting to its people and national identity.