'It's a jungle out there'?: Cloud computing, standards and the law

Niamh Gleeson & Ian Walden*

Cite as Gleeson N. & Walden I., "'It's a jungle out there'?: Cloud computing, standards and the law", in European Journal of Law and Technology, Vol 5, No 2, 2014.

ABSTRACT

Standards are a feature of all information and communication technology markets, including cloud computing. This article examines various strands of standards development in the cloud market, in respect of technical, informational and evaluative matters. It considers the concern expressed by the European Commission in 2012 that there was a 'jungle of standards' posing a potential barrier to cloud innovation and take-up, which was subsequently shown to be a misrepresentation of the current situation. The different policy objectives of standards-making are considered, specifically interoperability, data portability, data protection and data security. Current standards initiatives are outlined, focusing particularly in the area of evaluative standards, where cloud users are looking for assurances that their data is being processed in a secure and legally compliant manner. Recent work carried out by Commission-led expert groups in the areas of service level agreements and data protection; as well as international initiatives within the ISO/IEC are outlined. The interaction between standards and the law are analysed, from both a public and private law perspective. The article concludes that technical standards for cloud are progressing in a satisfactory manner; while it is in the area of evaluative standards that the greatest challenges lie, especially where the underlying legal framework is undergoing reform.

1. INTRODUCTION

Standards make the world go round. They embody a consensus about how to do something based on accumulated experience, as well as signalling how things should be done going forward. Standards are generally viewed as being a good as well as necessary thing; no more so than for the ICT sector, of which cloud computing is part. Yet, in September 2012, the European Commission identified a 'jungle of standards' as one of the key obstacles to the uptake of cloud, a barrier to market development with significant consequences for all stakeholders, especially small and medium enterprises (SMEs) and consumers;[1] not such a good thing! The debate raises a wider issue for policy makers in terms of what role standards can, and should, play in pursuing specific objectives and outcomes in the European cloud market.

This article focuses on EU initiatives on cloud standards, particularly the work of the European Telecommunications Standards Institute (ETSI), the European Union Agency for Network and Information Security (ENISA) and the working groups set up by the European Commission; while acknowledging that cloud standardisation is obviously

* Dr Niamh Gleeson and Professor Ian Walden are members of the Cloud Legal Project, in the Centre for Commercial Law Studies, Queen Mary, University of London.

[1] European Commission Communication, 'Unleashing the Potential of Cloud Computing in Europe' COM (2012) 529 final, Brussels, 27.09.2012 ('Commission Communication')..

also a global issue. It addresses three questions. First, we consider why standards play a role in cloud computing and examine the standards most cited as important for cloud computing: data protection, data security, interoperability, data portability, reversibility and service level agreements (SLAs). Second, we examine whether there is a problem with cloud standards and, in particular, the debate around the proliferation of cloud computing standards. We look at the factors that complicate adoption of appropriate cloud standards, including defining cloud standards, the standard-setting process for cloud and the variety of standards-setting organisations, governmental bodies and international organisations involved in developing standards for the cloud market.[2] Finally, we examine how the adoption of cloud standards can be granted, or acquire, legal and regulatory effects under both public and private law regimes, which impact on both providers and users of cloud services. We conclude that, while technical standards for cloud appear to be developing as expected, informational and evaluative standards will inevitably take longer to emerge and may require greater stability within the legal frameworks into which they are intended to operate.

2. WHY STANDARDS ARE IMPORTANT FOR CLOUD COMPUTING

Standards are important in cloud computing for a variety of reasons. Standards for interoperability and data and application portability can ensure an open competitive market in cloud computing because customers are not locked-in to cloud providers and can easily transfer data or applications between cloud providers. Standards for cloud security and for data protection in the cloud can reassure cloud customers that using the cloud is safe for them, their data and their businesses. Standards in these area build trust in cloud computing. Finally, standards concerning cloud metrics and service levels enable customers to evaluate and compare cloud providers, leading to more trust in cloud computing and more competition.

Below we outline the standards most frequently discussed in relation to cloud standards in the EU and explain why they could be important to cloud computing providers or customers.

2.1 CLOUD INTEROPERABILITY

Cloud interoperability describes the capability of different cloud ecosystems, operating across and within different layers of the supply chain, provisioned by different providers, to work together, interact and exchange instructions.[3] It includes the ability to exchange information between clouds according to a prescribed method and to obtain predictable results.[4] Interoperability implies that the cloud service operates according to an agreed standardised specification.[5]

In cloud services that involve Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) interoperability refers to the interfaces or APIs needed so that the virtualization platforms management interfaces operate between different providers. The ability for

[2] See further the section 3.2.2 below on standard-setting organisations for cloud.
[3] Hon and Millard, 'Control, Security and Risk in the Cloud' in C Millard (ed), *Cloud Computing Law*)(OUP, 2013), 26-27.
[4] European Telecommunications Standards Institute (ETSI),*Cloud Standards Coordination Final Report* (ETSI, November 2013) ('ETSI CSC Final Report'), 7.
[5] ETSI CSC Final Report, 7.

different clouds to work together is one feature of interoperability, but it also includes the ability to migrate workloads between different providers. In relation to SaaS, interoperability is more about compatibility of data formats, data files and protocols.

Interoperability standards are important for cloud providers so that multiple clouds can work together. For example, 'cloud bursting' describes a situation where multiple clouds have to work together, such as a private cloud of a company running virtual machines that need extra computation power from a public cloud (so called 'hybrid cloud solutions').[6] Interoperable standards are needed because of a coexistence of public and private cloud and the need to do some "offload" between them.[7] This allows cloud providers to operate together to offer more varied service offerings, to deal with outages and emergency cover and to give their customers greater flexibility and choice in the types of offerings.

From the point of view of cloud customers, the fear is that a lack of interoperability standards will lock-in users to proprietary infrastructure or platforms of customers or to certain data formats.[8] Without interoperable standards, investments in IaaS or PaaS are lost if customers migrate or try to switch providers. For this reason, cloud interoperability standards are important to ensure that customers at all levels of the service stack can switch providers or can migrate workloads to different providers easily.

To date, standards for cloud interoperability are still being developed.[9]

2.2 DATA PORTABILITY AND REVERSIBILITY

'Data portability' in cloud computing means the ability of users to recover the data supplied to, or generated by, the cloud service, including metadata and associated applications, and to move them between multiple cloud providers at low cost and with minimal disruption.[10] There are several aspects to data portability, but generally data portability means that the data are recoverable in formats that are easily accessible, readable and importable into either internal applications or another provider's cloud.[11] This is particularly important for Software as a Service (SaaS) where the model is focussed on individual end-users, mainly consumers or SMES, who may not be aware of the pitfall of not being able to move seamlessly from one vendor to another when they sign up for the service.

The need for data portability standards is driven by a concern that there is a risk of customers becoming overly dependent on one cloud provider's service, and the potential inability of users to switch between service providers (or 'lock-in'), which could have a negative impact on competition in the cloud market.[12]

---

[6] This is the use case described in the ETSI CSC Final Report at 11.
[7] ETSI CSC Final Report, 11.
[8] European Committee for Interoperable Systems (ECIS), *Cloud Computing Standards Compatibility and Interoperability: Ensuring a thriving and competitive market*, 13 November 2014.
[9] For example SNIA's Cloud Data Management Interface (CDMI) standard adopted by ISO 17826:2012. Referenced in the ETSI CSC Final Report.
[10] ETSI CSC Final Report, 7.
[11] Hon and Millard, 26.
[12] See Walden, I. and Laíse Da Correggio Luciano 'Facilitating Competition in the Clouds', in C Millard (ed), *Cloud Computing Law*, (OUP, 2013), 327-328.

Standards have already been developed with respect to enabling data portability, both generic for web-based environments,[13] which would include cloud, as well as specifically for cloud environments.[14] In addition, some cloud providers have developed initiatives designed to facilitate portability into and from their services, such as Google's 'Data Liberation Front' and its provision of 'Takeout' information; although it has since become part of its standard support service.[15] For other providers, such as AWS[16] and Microsoft[17], data portability forms one component of a broad cloud interoperability offering.

Reversibility can be defined as the ability to move data into and out of cloud since many users are likely to operate 'dual' cloud and non-cloud systems for the foreseeable future.[18] It is therefore related to attempts to prevent 'lock-in' by allowing users to withdraw data from Cloud, and is closely related to data portability. To date there does not appear to be any standard or draft specification on reversibility in cloud[19] and it seems unlikely that this can be considered as a separate standard from data portability.

2.3 DATA PROTECTION STANDARDS

Data protection laws regulate the processing of personal data and have significant implications for cloud computing.[20] The legal requirements imposed by data protection law are divided between the cloud service provider and its customers and vary according to legal jurisdiction, and according to the terms of the contract between the cloud service provider and the customer.

Cloud service providers who process personal data under contract to their customers have to operate their services in ways that allow both parties to meet the requirements of applicable legislation and regulations covering the protection of personal data. The obligations may depend on whether the cloud provider or cloud customer is a data processor, processing data on behalf of others, or also a data controller, with authority over the processing and use of the data. Therefore demonstrating compliance with data protection laws for all jurisdictions has become an increasing concern for cloud providers and customers. It was particularly a concern to build trust in their service and trust in how they dealt personal data.

[13] E.g. the Open Data Protocol, 'OData', which was approved as an OASIS international standard in March 2014, see https://www.oasis-open.org/news/pr/oasis-approves-odata-4-0-standards-for-an-open-programmable-web

[14] E.g. DMTF Open virtualization Format Specification V2 (DSP0243), which enables the porting of VMs, also OASIS/TOSCA Topology and Orchestration Specification for Cloud Application, see ETSI CSC Final Report, Annex 1 and p.32.

[15] https://support.google.com/accounts/answer/3024195

[16] https://aws.amazon.com/importexport/

[17] http://cloudinteropelements.cloudapp.net/data-portability.aspx

[18] Industry Recommendations to Vice President Neelie Kroes on the Orientation of a European Cloud Computing Strategy, November 2011. Accessed at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendations-ccstrategy-nov2011.pdf.

[19] It is not referred to in the ETSI CSC Final Report, even though this was one of the 'necessary standards' referred to by the Commission in its request to ETSI in Commission Communication, 10.

[20] This is covered in detail in Part III, Chapters 7-10, in C Millard (ed), *Cloud Computing Law*,(OUP, 2013).

In response to the increasing use of cloud, the ISO/IEC has published a new standard specifically for the use of public clouds as data processors.[21] The aim of the standard is to create a common set of security controls that can be implemented by a public cloud service provider that is processing personal data on behalf of another party. Organisations can use the standard to select applicable controls when implementing a cloud computing information security management system or guidance; although the standard does not specify what controls are applicable to what organisation and instead requires a risk assessment to be performed to identify what controls are required. The importance of this standard is that cloud providers can confirm compliance with important data protection standards and a self-audit by a provider can be accepted as proof of compliance with technical and organisational measures required, for example, under EU data protection directive.[22]
Most of the controls in the standard will apply to data controllers, although they are subject to additional controls not set out in the standard, which specifically references data processors only.

The standard broadly addresses the key obligations in data protection and privacy laws around the world, but the standard cannot claim to address all the specific differences in every data protection law worldwide. Therefore, cloud providers and cloud customers still have to consider legal compliance and not just compliance with the standard. In addition, specific industries have specific data protection rules relevant to their sector, for example, the health sector or the financial services sector.[23] The standard does not address sector-specific rules or concerns.

Nevertheless, this standard goes some way to providing reassurance that the cloud processor is using best practice as given by an international standard-setting organisation, the ISO, and thus, by implication reassuring customers. It is the first global standard on this topic and provides a useful reference for customers and suppliers alike.

2.4 CLOUD SECURITY STANDARDS

Security concerns are identified as one of the main challenges when it comes to building trust and confidence in cloud computing services.[24] Challenges and risks particular to cloud security are identified in several studies.[25] References to cloud security include

[21] ISO/IEC DIS 27018, 'Code of practice for PII protection in public cloud acting as PII processors', see http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498 . ISO/IEC 27018 First edition 2014-08-01, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
[22] Article 17 of Directive 95/46/EC 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 [1995] OJ L 281, 23.11.1995, 31-50 (the Data Protection Directive or DPD).
[23] For example, in the US the *Health Insurance Portability and Accountability Act* of 1996 (*HIPAA*) and the financial privacy provisions of the *Gramm-Leach-Bliley Financial Modernization Act* of 1999. The GLB Act requires companies to give consumers privacy notices that explain the institutions' information-sharing practices.
[24] IDC (2012) 'Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up' referenced in the Commission Communication and the accompanying Staff Working Document.
[25] Such studies include ENISA 'Benefits, risk and recommendations for cloud security' November 2009, at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment; Cloud Security Alliance 'The Notorious Nine: Cloud Computing Top Threats in 2013' February 2013, at: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Comp

network and information security in general and are broader than purely protection of personal data. Concerns about cloud security extend to infrastructure resilience, authentication,[26] certification of processes and protection against illegal activities in the cloud environment including malicious system or data interference to the cloud users or service providers.[27] Concerns about the protection of personal data, the problem of data breaches and protection against cyber-attacks are not unique to the cloud environment but the difference from traditional ICT outsourcing is that there is a greater loss of control by the cloud user. In addition, cloud may involve the sharing and delegation of control amongst the various layers of service providers, often opaque to any one of them; and the cloud provider operates an environment in which resources are shared (the multi-tenant cloud model).[28]

The variety of proposed security standards, with varying degrees of maturity, as well as a lack of clarity around the suitability of certification schemes, has been found detrimental to building trust in cloud services.[29] An ISO standard on security for cloud computing services is under development and is supposed to be published in 2015.[30]

2.5 STANDARDISED SERVICE DESCRIPTIONS AND SLAS

SLAs, and particularly standardised service descriptions and consistent and comparable service terminology, have been a feature of calls for standards in cloud.[31] Without standardised descriptions of cloud services, buyers may find it difficult to understand what they are buying and cannot easily compare services or determine the relative value of offerings. Such informational standards can be seen as a demand-side measure designed to facilitate competition in the cloud market; although according to the Commission, it is also a concern for building trust in cloud services. The development of model terms for SLAs was one of the most important issues that arose from its consultation on cloud strategy.[32]

Service level targets for cloud need to be well-defined, so that cloud suppliers should not be able to interpret measures differently; determinate, so that multiple measurements of identical systems in identical states must give the same result; correlated to business value or to real-world performance of typical consumer tasks; and comparable, so that metrics reflect the same quantity across different measurement targets.[33] The value of

---

uting_Top_Threats_in_2013.pdf; Cloud Standards Customer Council ' Security for Cloud Computing' August 2012, at https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[26] Commission Communication, 7. The Commission refers to the need for secure eAuthentication methods for Internet transactions since reliable authentication is necessary in cloud because of the complex value chains of many services in cloud computing.

[27] Commission Communication, 6.

[28] Hon andMillard 'Control, Security and Risk in the Cloud' Chapter 2 in C Millard (ed), *Cloud Computing Law*(OUP, 2013), 27.

[29] ETSI CSC Final Report, 8.

[30] ISO/IEC CD 27017 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud computing services, accessed at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757

[31] In Commission Communication, at 11, but see also the US Government Cloud Computing Technology Roadmap Requirements Volume I, November 2011, which identifies 'High quality service-level agreements' at 17. Also private standards development organisations like the Cloud Standards Customer Council 'Practical Guide to Cloud Service Level Agreements', April 10 2012. Accessed at: http://www.cloudstandardscustomercouncil.org/2012_Practical_Guide_to_Cloud_SLAs.pdf

[32] Commission Communication, 11.

[33] ETSI CSC Final Report, 7.

comparable metrics has already been recognised in the telecommunications sector, as well as other utility markets, and an obligation to supply appropriate data can be mandated for providers.[34]

3. PROBLEM IDENTIFIED WITH CLOUD STANDARDS

Several factors complicate the standard-setting environment for cloud standards, including the number of standards bodies involved in cloud standards and the definition of 'cloud standard.' Consequently there is a prevailing concern that cloud standard-setting is flawed or problematic. This section examines these concerns and analyses whether they are justified.

3.1 THE PROBLEM: TOO MANY OR TOO FEW CLOUD STANDARDS?

Many commentators have highlighted the proliferation of cloud standards and expressed concern about their development.[35] One author describes emerging cloud standards as 'an alphabet soup of complex, over-lapping specifications from too many organizations.'[36] In September 2012, the European Commission weighed in on this debate and identified a 'jungle of standards' as one of the key obstacles to the uptake of cloud, a barrier to market development with significant consequences for all stakeholders, especially small and medium enterprises (SMEs) and consumers.[37]

The first policy concern expressed by the Commission was that industry would not agree to standards for interoperability and data portability. According to the Commission, industry players are fighting for dominance, which inhibits standardisation, and consequently cloud may develop in a way that 'lacks interoperability, data portability and reversibility, all crucial for the avoidance of lock-in'.[38] In other words, its fear is that cloud providers do not want to be interoperable, and that a situation where there is no interoperability or data portability between cloud providers could lead to customers being locked-in or unable to switch from their cloud provider. The Commission therefore advocates technical standards that set out protocols for interoperability and data portability in the cloud.

The second main policy concern expressed by the Commission is that more cloud standards are needed in areas concerning data security and data protection to ensure cloud take-up. The Commission argues that trust in cloud solutions starts with 'the identification of appropriate standards that can be certified to allow public and private procurers to be confident that they have met their compliance obligations and that they

[34] For telecommunication providers, see Directive 2002/22/EC on 'universal services and users' rights relating to electronic communication networks and services' (as amended), at article 22(2). For other utilities, see the Enterprise and Regulatory Reform Act 2013, ss. 89-91.
[35] For example see Sixto Ortiz Jr., 'The Problem with Cloud-Computing Standardization' *Computer* (July 2011) Vol 44, Issue No 7, pp 13-16, magazine published by IEEE magazine available at: http://www.computer.org/portal/web/computingnow/computer and N. Borenstein and J. Blake, 'Cloud Computing Standards: Where's the Beef?' (2011) 15 *Internet Computing*, IEEE 74.
[36] In Baudoin 'Cloud Standards? It's the Users' (2012) 25 *Cutter IT Journal* 22-28.
[37] European Commission Communication, 'Unleashing the Potential of Cloud Computing in Europe' COM (2012) 529 final, Brussels, 27.09.2012 ('Commission Communication').
[38] Commission Communication 10.

are getting an appropriate solution to meet their needs when adopting cloud services'.[39] Standards and certification can then be used in contracts so that providers and users can define rights and liabilities by reference to them.[40] Since users are rarely able to evaluate suppliers' claims about implementation independently, it finds that trusted certification is needed.[41]

Therefore the spectrum of concern about cloud standards ranges from fears that there are potentially too many competing standards (for example, standards based on proprietary software used for interoperable applications and data formats) and concerns that there were too few standards adopted by the cloud computing industry, (for example for data protection and data security).

3.2 FACTORS COMPLICATING THE DEBATE ON CLOUD STANDARDS

The debate on cloud standards is complicated by two particular factors. First, a 'cloud standard' can mean a variety of different measures, and calls for 'cloud standards' can consequently lead to a range of different outcomes. Second, there are numerous organisations simultaneously developing cloud standards. Identifying these organisations and assessing what they are developing (and whether they are overlapping) is a difficult task for cloud providers and cloud customers.

3.2.1 WHAT IS MEANT BY "CLOUD STANDARD"?

A factor in the debate on cloud standards arises from use of the term 'standard' to encompass a confusingly diverse range of subject matter. The standards discussed for cloud computing can broadly be categorised into three types: technical, informational and evaluative.

- ***Technical standards*** – specify the 'gory details' of a format, protocol, or interface and describe how to make things works in an interoperable manner.[42] For example, in cloud computing technical standards cloud be used to define interoperable interfaces between different cloud providers.
- ***Informational standards*** – set the parameters for types of information or metrics that can be used to communicate information about a product or service.[43] Guidelines on 'standardised' attributes for cloud Service Level Agreements (SLAs)[44] have become a focus for a variety of bodies involved in cloud standards.[45] Organisations have focussed on standardising SLAs to provide meaningful comparisons between, and evaluations of, competing cloud vendors.[46]

[39] Commission Communication 9
[40] Commission Communication 9
[41] Commission Communication 10
[42] N. Borenstein and J. Blake, 'Cloud Computing Standards: Where's the Beef?' (2011) 15 *Internet Computing*, IEEE 74.
[43] Organization for Economic Cooperation and Development (OECD) 'OECD Policy Roundtable on Standard Setting' DAF/COMP (2010) 33.
[44] An SLA describes the level of service expected by a customer from a service provider. It provides information on the contracted services and their expected reliability and provides metrics for measuring the service and the remedies or penalties if the agreed-upon performance levels are not achieved.
[45] One of the actions on standards identified by the European Commission is to 'Develop with stakeholders model terms for cloud computing service level agreements for contracts between cloud providers and professional cloud users' (Commission Communication at 12).
[46] E.g. proposed ISO standard ISO/IEC 19086 'Cloud computing – SLA framework and terminology'.

- ***Evaluative standards*** – tests and certifies the proper use of best-known practices.[47] Evaluative standards are seen as a means of enabling cloud users to assess service providers and their service quality including, for example, uptime, performance, availability, security, privacy, compliance, and portability across cloud providers.[48] Unlike technical standards, where compliance can be measured objectively, evaluative standards often depend on third-party certification to demonstrate compliance.

In addition, a standard is more than a document with a fixed description of a technical specification. The phrase 'standards as a process' has been used to describe the development of ICT standards,[49] which reflects the fact that a standard will need to evolve and adapt as the underlying technologies evolve. Such evolutionary pressures are inevitably more evident in the field of technical standards. By contrast, for evaluative standards, a certain degree of stability and certainty is obviously more desirable, in order for them to achieve their purpose of engendering trust and encouraging reliance.[50]

Consequently, referring to 'cloud standards' in policy debates can mean a wide variety of different measures, each with different functions, public policy implications and legal effects.

3.2.2 ORGANISATIONS DEVELOPING CLOUD STANDARDS

There are several potential sources of standards: standards created by official international, regional or national standard-setting bodies, private standard-setting organisations, government-imposed standards and standards arising from market forces;[51] while different sources may simultaneously be developing competing standards. The sources involved in developing cloud computing standards covers the full range of types of organisations that are sources of standards.[52] The most important for the purposes of this article are the EU initiatives on cloud standards.

3.2.2.1 European Union initiatives

The EU has several initiatives that impact on standards in cloud computing. Following the publication of its cloud strategy communication, the European Commission has tasked several bodies with work relevant to cloud standards:[53]

---

[47] Borenstein and Blake (2011) .
[48] The Commission Communication call for 'a detailed map of the necessary standards' for cloud which it describes as 'inter alia for security, interoperability, data portability and reversibility.' (at 10).
[49] David R. Bernstein, 'A Standard Isn't a Document - It's a Process' (2012) 25 *Cutter IT Journal* 17–21
[50] Characteristics not dissimilar to those associated with the concept of the 'rule of law' Raz, J., "The Rule of Law and its Virtue" [1997] 93 *LQR* 195.
[51] OECD Policy Roundtable on Standard-Setting (2010), pp 23-25.
[52] Both the ITU and ETSI have tried to map the range of organisations involved in various areas of development of cloud standards. See Report by ITU-T FG Cloud TR 'Focus Group on Cloud Computing Technical Report Part 6: Overview of SDOs involved in cloud computing' 02/2012; and Report by ETSI providing an overview of the standardisation organisations and their activities related to Cloud computing. CSC – TG3 List of Cloud SDO activities, 10 May 2013.
[53] Detailed in the document 'Brochure: Working groups for the implementation of the Cloud Computing Strategy' dated 19 March 2013 which sets out a diagram showing the working groups, their relationship with key actions in the Commission cloud strategy and the launch date of each working group. Accessed at https://ec.europa.eu/digital-agenda/en/news/working-groups-implementation-cloud-computing-strategy.

- ***Mapping cloud standards –*** The European Commission has tasked the European Telecommunications Standards Institute (ETSI) to map cloud standards, meaning to report on cloud standards. In response to the Commission's call to action, ETSI established a Cloud Standard Coordination group and in late 2013 published a report on the actual status of cloud standards.[54] Its report on cloud standards is assessed in detail in the next section below.
- ***Cloud Select Industry Group on cloud computing -*** The Cloud Select Industry Group (C-SIG)[55] is a working group set up by the European Commission to deal with various cloud computing issues. There are three sub-groups: one working group focuses on SLAs for cloud computing, one focuses on data protection in cloud computing and one focuses on certification for cloud computing. These work with industry to agree on norms for different aspects of cloud service. The Cloud Select Industry Group on developing cloud computing Service Level Agreements deals with contracts between cloud providers and enterprise cloud users.[56] In June 2014, this group published its guidelines aimed at business cloud customers, the Cloud Service Level Agreements Standardisation Guidelines.[57] The guidelines set out a series of service level objectives covering essential elements of the SLA including availability and reliability of cloud service, security reliability, data management and personal data protection. The standardisation guidelines provide a starting point for a business customer to understand and compare cloud offerings. In the preamble to the guidelines, they acknowledge that the initiative will have maximum impact only if done at the international level rather than purely at the regional level and, to this end, the guidelines form the basis for the submission by the C-SIG SLA subgroup as the European Commission expert group to the ISO/IEC JTC 1 Working Group on Cloud Computing which is currently working on an international standard for Cloud SLAs. [58]
- ***European Commission Expert group on Cloud Computing Contracts –*** This is a European Commission initiative from DG Justice that deals with terms and conditions in cloud computing contracts between service providers and consumers and small firms.[59] Although the task of this group is supposed to be complementary to the work on model terms by the Cloud Select Industry Group on SLAs,[60] its membership is different,[61] its focus is slightly different, but the scope of the work is

[54] ETSI CSC Final Report.
[55] There is no formal Commission decision setting up the Cloud Select Industry group and its sub-groups, although it is linked to the Directorate General for the Information Society ('DG Connect') and meetings and minutes of the working groups are set out on the DG Connect website.
[56] https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-service-level-agreements on 10 January 2014.This group interfaces with the ETSI group mapping standards for SLAs see Report of the first meeting of the Cloud Select Industry Group – Service level agreement expert subgroup held on 21st of February 2013, p.2. Accessed at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/22022013%20Report_1%20SLA%20group.pdf. The website of ETSI Taskgroup on SLAs is available here: http://csc.etsi.org/website/home.aspx
[57] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines
[58] ISO/IEC JTC1/SC38 at http://www.iso.org/iso/iso_technical_committee.html?commid=601355 and http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63902
[59] Commission Decision of 18 June 2013 on setting up the Commission expert group on cloud computing contracts (2013/C 174/04), OJ C174/6, 20.06.2013. "Commission Decision expert group 2013)
[60] Commission Decision expert group 2013, recital 5.
[61] Commission Decision expert group 2013, art. 5. Its members include experts on data protection relevant to cloud computing, European and national umbrella organisations, business providing cloud computing services, representatives of cloud computing customers, representatives of the legal profession and academia and representatives of the European Commission. See the Commission

so similar, it seems likely that having two different groups managed by two different parts of the European Commission dealing with cloud terms and conditions could result in potential duplication of work, at best, or conflicting results at worst. It is likely to result in a 'jungle of groups' rather than a 'jungle of standards'!

- ***European Union Agency for Network and Information Security (ENISA) and the working group on certification schemes***[62] – The Commission Communication proposed as an action that to assist in development of EU-wide voluntary certification schemes there should be a list of such schemes.[63] It tasked ENISA to support this work. To further the work on cloud strategy, the European Commission also set up a group of experts from industry, called the Cloud Select Industry working group on Certification (CERT-SIG). This sub-group had as its scope certification schemes for data protection, but extended this to certification schemes for security too in its first meeting.[64] ENISA has worked with CERT-SIG and published a list of certification schemes arising from this work and its own analysis of this and its recommendations for future actions on voluntary certification schemes for cloud standards.[65]

3.2.2.2 Official standard-setting organisations

All the official international standards organisations[66] are involved in work on developing cloud computing standards. The International Telecommunications Union (ITU) has a Cloud Working Group and several study groups working on various aspects of cloud standards.[67] The International Standards Organization (ISO) and International Electro-Technical Commission (IEC) are involved in cloud computing jointly via a Joint Technical Committee (JTC1) which is developing recommendations on cloud computing terms and definitions and cloud computing reference architecture to produce an

---

Register of Expert Groups accessed at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailPDF&groupID=2922.

[62] To date however, they appear to be working closely together. See press release 25 February 2014, ENISA 'Supporting the activities of the EU Cloud Strategy, ENISA has published a list of the existing Cloud Certification schemes. This will help potential cloud users decide on the security of different cloud solutions. The list was developed by ENISA in close collaboration with the European Commission and the private sector (the CERT-SIC – the certification working group) at http://www.enisa.europa.eu/media/news-items/enisa-takes-a-step-forward-in-building-trust-in-the-cloud

[63] Commission Communication, 11. There is also a parallel initiative on mandated audit and certification, under the Commission's proposed directive on network and information security (February 2013).

[64] Output of CERT SIG group as reported by ENISA in 'Certification in EU Cloud Strategy' in November 2013, 2.

[65] ENISA 'Certification in EU Cloud Strategy' November 2013: https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy/at_download/fullReport.

[66] See S. Kurihara 'Foundations and Future Prospects of Standards Studies' (2008) *J of IT and Standardization Research* 6(2), 1-20 July-December 2008.

[67] ITU work on cloud standards includes reports and white papers published by various of its Focus Groups (FG) on Cloud: FG Cloud Part 1 has published 'Introduction to the cloud ecosystem'; FG Cloud Part 2 'Functional requirements and reference architecture'; FG Cloud Part 3 'Requirements framework architecture of cloud infrastructure'; FG Cloud Part 4 'Cloud Resource Management Gap analysis'; FG Cloud Part 5 'Cloud security'; FG Cloud Part 6 'Overview of SDOs involved in cloud computing'; FG Part 7 has published 'Cloud benefits from telecommunications & ICT perspectives' and draft standards 'Cloud Computing overview and vocabulary', 'Framework on inter-cloud', 'Cloud computing Reference Architecture'.

internationally-agreed standard for discussing cloud computing.[68] It has working groups for cloud standards dealing with topics such as information security management, risk management, application and network security, cybersecurity, and business continuity.[69]

In addition to the international standards organisations, regional and national standards organisations are involved in cloud standards. In Europe, the various groups involved in cloud standards have been outlined above. At national level, there are official standards organizations in all industrialised countries that represent their countries in the ISO or IEC.[70] In the US, the National Institute of Standards and Technology (NIST), a non-regulatory agency of the US Department of Commerce, is an example of a national standards organisation that has significant international influence through its work on cloud standards.[71]

3.2.2.3 Private standard-setting organisations

Standards organisations where national governments are not members are defined as private standard-setting organizations and include private consortia or industry fora that develop standards. A wide range of private standard-setting bodies are contributing to the development of standards for cloud. The ITU has issued a report giving an overview of the range of organisations involved in cloud computing[72] and ETSI has produced a similar report with a list of standardisation organisations and their activities related to cloud computing.[73]

Many of the same organisations appear in both the ITU and ETSI reports and some of their initiatives have led to the adoption of cloud computing standards. Two private organisations in particular have produced standards that have been adopted by the ISO/IEC as cloud standards. A non-profit private industry organisation involved in cloud computing standards for interoperability, the Distributed Management Task Force (DMTF), created the open virtualisation format (OVF) which enables the secure packaging and portability of virtual machines between clouds which is essential to the interoperability of IaaS clouds. OVF was adopted by the ISO/IEC in 2011.[74]

The Storage Networking Industry Association (SNIA) is an association with the goal of promoting acceptance and confidence in storage architecture, system and service technologies. It has produced the Cloud Data Management Interface (CDMI) as a

[68] Published standards are: ISO/IEC 17203 OVF and ISO/IEC 17826 Cloud Data Management Interface (same as SNIA CDMI). Draft standards include ISO/IEC 17788 Cloud Computing Overview and Vocabulary; ISO/IEC 17789 Cloud Computing Reference Architecture; ISO/IEC 27017 Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002; ISO/IEC 27018 Code of practice for data protection controls for public cloud computing services; ISO/IEC 19086 Cloud computing – SLA framework and terminology.
[69] ITU published standards.ISO/IEC 17203 OVF and ISO/IEC 17826 Cloud Data Management Interface.
[70] Although national standardisation work has significantly decreased the national organisations play an important role in transposing international or regional standards into national standards. R. Werle 'Institutional aspects of standardisation – jurisdictional conflicts and the choice of standardisation organizations' (2001) *Journal of European Public Policy* 8:3, 392-410, at 396.
[71] For example the NIST definition of cloud computing is widely cited. See 'The NIST Definition of Cloud computing. Recommendation of the NIST Special Publication 800-145 (P. Mell and T. Grance).
[72] Report by ITU-T FG Cloud TR 'Focus Group on Cloud Computing Technical Report Part 6: Overview of SDOs involved in cloud computing' 02/2012.
[73] Report by ETSI providing an overview of the standardisation organisations and their activities related to Cloud computing. CSC – TG3 List of Cloud SDO activities, 10 May 2013.
[74] ISO/IEC JTC 1 SC38 approved OVF v1 as an ISO standard (ISO/IEC 17203:2011).

standard that defines an interface for interoperable transfer and management of data in a cloud storage environment and this was adopted by the ISO/IEC as a standard in 2012.[75]

Over 20 private organisations are identified as involved in cloud standards by the ITU and ETSI. Even those involved in the same standardisation issues are often involved from differing perspectives, whether driven by providers or users; although the former tend to dominate. Therefore, the impression that there is a wide range of differing or even competing standards organisations all involved in arriving at a 'cloud standard' is misleading, since most of these organisations are not in fact developing competing, but complementary standards, or standards on widely differing cloud-related issues.[76]

3.2.2.4 Government-imposed standards

Government involvement in standard-setting can be as active participants in standard organisations, or as a registration and enforcement service for standards by imposing regulatory or legal obligations that include standards. Some governments have directly set standards for issues related to cloud. Singapore, for example, has launched a cloud security standard.[77] Most government strategies however do not involve standard-setting or standard design, but more indirectly involve the support of standards as necessary for cloud take-up.[78]

The role of governments in cloud standard-setting processes is also as a customer and potentially the largest buyers of IT services and, by exercising their buyer power as ICT customers, they can be key in developing cloud standards. Many national governments in adopting a cloud strategy have adopted a cloud policy for their procurement decisions and consequently governments can set criteria for features, performance, security and standards for cloud services. One of the European Commission's actions as part of its cloud strategy[79] is to promote common public sector leadership on cloud services by setting up a European Cloud Partnership (ECP) to bring together industry expertise and public sectors users to work on common procurement requirements for cloud computing. The ECP will identify public sector cloud requirements, develop specifications for IT procurement and advance towards joint procurement of cloud computing services by public bodies.[80]

The role of governments in standard-setting has been argued to be more objective and less anti-competitive than private standard-setting initiatives.[81] Nevertheless, the

[75] ISO/IEC 17826 Cloud Data Management Interface (same as SNIA CDMI).
[76] This is one of the conclusions of the ETSI exercise on mapping of cloud standards in its ETSI CSC Final Report.
[77] Standard MTCS SS (SS 584) 'Specification for multi-tiered cloud computing security' (2013, Infocomm development authority of Singapore). The SS 584 is a cloud security standard that covers multiple tiers and can be applied by Cloud Service Providers (CSPs) to meet differing cloud user needs for data sensitivity and business criticality and it allows certified CSPs to spell out the levels of security that they can offer to their users. Accessed at http://www.ida.gov.sg/Infocomm-Landscape/ICT-Standards-and-Framework/MTCS-Certification-Scheme.
[78] Countries around the world are developing overarching strategies that are designed to encourage cloud uptake. Examples of various national cloud strategies are China's 12th Five-Year Plan (it includes $174 million to develop cloud computing hubs in the PRC); the Cloud Computing Strategic Direction Paper in Australia and similar initiatives in New Zealand, Singapore and Malaysia; France's Andromede program, Germany's Trusted Cloud; and the UK's G-Cloud initiative.
[79] Commission Communication, at 13.
[80] Commission Communication. 14
[81] C. Koenig and K. Spiekermann, 'EC competition law issues of standard setting by officially-entrusted versus private organisations' (2010) 31 *European Competition Law Review* 449–458

deliberate interference by government in the development of national and international standards to pursue national security goals could undermine trust in cloud. For example, it was recently revealed that the US National Security Agency (NSA) influenced cryptographic standards with a surreptitious 'backdoor' for the NSA.[82] Revelations like this have contributed to an environment where uncertainty about the security of cloud services is further undermined by mistrust regarding government access to information held in the cloud.[83]

3.3 ANALYSIS OF WHETHER THERE IS A PROBLEM WITH CLOUD STANDARDS

The number of organisations involved in standard-setting and the range of measures that could possibly count as 'cloud standards' means that assessing whether there is a proliferation of competing standards is a difficult task. Nevertheless, in order to decide whether there is a problem with cloud standards, it is necessary to identify in what areas there are too few or too many standards.

3.3.1 MAPPING CLOUD STANDARDS

In response to the Commission's call to action, the European Telecommunications Standards Institute (ETSI) established a Cloud Standard Coordination group and in late 2013 published a report on the actual status of cloud standards.[84] This gave a helpful and enlightening synopsis of adopted and draft standards on cloud computing and the organisations involved in developing the standards.

The bulk of the report consists of what ETSI calls 'technical results': a collation of lists of standards and specifications related to cloud, a list of organisations producing these standards and specifications, a list of the white papers and reports produced by standards organisation relevant to cloud, and a mapping of these documents onto the activities that need to be undertaken by cloud service customers or cloud service providers over the whole cloud service life-cycle.[85] This is intended to be a status report on the current state of cloud standardisation. Based on these lists and mapping, the report draws conclusions concerning the current state of cloud standardisation. It arrives at three conclusions, some of which are surprising.

3.3.2 ASSESSMENT OF THE CURRENT STATUS OF CLOUD STANDARDISATION

The ETSI report concludes that while the cloud standards landscape is complex, it is neither chaotic nor a 'jungle',[86] and instead describes it as a 'dynamic landscape'.

---

[82] New York Times article http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/ or NIST announcement about removing the cryptographic algorithm standard concerned from its draft guidance http://www.nist.gov/itl/csd/sp800-90-042114.cfm. Mike Masnick 'Details Reveal Crypto Standard Controlled by NSA' September 11 2013, accessed at http://www.techdirt.com/articles/20130911/10302624487/details-reveal-crypto-standard-controlled-nsa-how-canada-helped.shtml Having successfully authored the standard, the NSA then tried to push the same standard on the ISO, again without the knowledge of those involved in the standards process

[83] See Walden, I., 'Law enforcement Access to Data in Clouds', Chapter 11 in *Cloud Computing Law* (ed. Millard)(OUP, 2013).

[84] ETSI CSC Final Report.

[85] ETSI CSC Final Report, Executive Summary.

[86] ETSI CSC Final Report, Executive Summary and Conclusions.

Focussed Standardisation

The report finds that cloud standards and specifications are in general not overlapping but are addressing specific, but different, issues in the cloud life-cycle. In its analysis of 'Use Cases', ETSI identifies a relatively small number of generic or specific activities that are undertaken across the whole 'life-cycle' of the cloud service. It finds that 'the number of relevant standards in a given activity is rarely above 2'.[87] It concludes that cloud standardisation is focussed. It seems, there are few activities where there are more than two competing standards addressing the same area of activity, even though the number of organisations and documents involved all with the title of cloud standard or specification might seem overwhelming to the uninitiated observer.

Maturity and adoption

The second main conclusion of the ETSI report is that given its dynamism, cloud standardisation will mature as new standards for technology are needed and that this will happen during 2014-2015.[88] It suggests that the reason why cloud standards are not seeing widespread adoption is because the 'standards' are only written to suit certain providers and 'are not flexible enough to be adopted by a wider community'. Thus some 'standards' are not in fact standards in the true sense, since they only suit particular cloud providers. Second, the report suggests that cloud standards may emerge from open source projects that are 'creating tried-and-tested APIs, protocols and environments which address aspects of interoperability, portability and security relating to cloud computing'. While acknowledging that these developments 'should be encouraged', it notes that the role of open source projects was not addressed in the report. The omission of open source indicates how incomplete the report is as a survey of cloud standards, yet it gives no explanation for why its scope omitted open source. Finally, given the recent incident concerning OpenSSL and the 'Heartbleed' vulnerability,[89] cloud users may feel less trusting of open source solutions as 'tried-and-tested'!

Coverage and gaps

The third conclusion of the report is that there are important gaps in the cloud standards landscape. It states that new cloud computing standards or extensions to existing standards that fill this gap should be encouraged.[90] The gaps it identifies are predictably in standards for interoperability, security and privacy. More interestingly, it identifies a need for an agreed set of terminology and definition for service level objectives in SLAs.[91] In addition, it identifies 'regulation, legal and governance' aspects as gaps in the cloud standardisation landscape and concludes that 'the legal environment for cloud computing is highly challenging and a key barrier for adoption'. The report doesn't specify which legal rules, but presumably means those relating to data privacy and security. It concludes with a sweeping statement that 'there is a need for international Framework and Governance, underpinned via global standards'.[92]

---

[87] ETSI CSC Final Report, Conclusions, at 34.
[88] ETSI CSC Final Report, Conclusions.
[89] CVE-2014-0160 & OpenSSL v.1.0.1-1.0.1f. See http://heartbleed.com/. However, Heartbleed has at least spurred the tech industry to 'fund open source projects that are in the critical path for core computing functions' (broader than cloud computing): http://www.linuxfoundation.org/programs/core-infrastructure-initiative.
[90] ETSI CSC Final Report, Conclusions.
[91] This indicates that the work of the Cloud Select Industry Group on SLAs and the Expert Group on cloud contracts work (discussed earlier in this section) is as important as the work on technical standards on interoperability.
[92] For a discussion on cloud governance see Chris Reed 'Cloud Governance: The Way Forward', in *Cloud Computing Law* (ed. Millard)(OUP, 2013) pp 362-389. Reed discusses how such governance frameworks should emerge rather than be imposed.

3.3.3 CONCLUSION ON CLOUD STANDARDS MAPPING

The ETSI report concludes that the problem with cloud standards is not that there is a jungle of competing technical standards, but that there is a need for more work on technical standards, which is progressing, although gaps remain. The ETSI report also highlights concerns with the variety of initiatives on security standards, designed to reassure users, and the difficult legal and regulatory framework surrounding security and privacy. This legal framework inhibits adoption of cloud security standards. From the range of organisations listed by ETSI, it appears that all major standards organisations are taking initiatives in this area but no single 'security' standard has yet emerged[93] although ISO/IEC is likely to emerge soon.

Therefore, the legal concerns that appeared to trigger the European Commission strategy paper, primarily to do with concerns about competition in the cloud market being stifled by a lack of interoperability standards, do not appear to match reality. Instead, the lack of interoperability standards takes second place to the more pressing concern of providing a framework for security and privacy standards that reassures users about cloud security. It suggests that the most pressing legal issues with cloud standards can only be resolved by agreed global standards on security and data privacy.

4. STANDARDS AS LAW

If standards matter as a tool of public policy, then questions of legal effect will inevitably follow: what does it mean when a cloud provider 'adopts' a standard? What are the legal and regulatory consequences of compliance with a standard, or more importantly, non-compliance?

Standards may be 'adopted' voluntarily, negotiated or mandated on a cloud provider, or the sector as a whole, through both public and private law mechanisms. Public law mechanisms can range from legislative requirements to regulatory guidance, with the potential for criminal or administrative sanctions. Private law refers primarily to contractual agreements, although it could extend to private law remedies such as breach of confidence, negligence, or other tortious or equitable claims for relief. Technical standards generally develop through industry initiatives and therefore tend to reside more in the realm of private law and self-regulation; although as Lessig has noted, their impact in terms of regulating our behaviours may be just as significant as traditional laws and regulations.[94] Informational and evaluative standards are more likely to involve and directly impact a wider range of stakeholders and are often taken up by legislators and regulators as part of the response to a policy concern. The following section examines some of the different means by which standards can be given legal effect.

4.1. PUBLIC LAW AND CLOUD STANDARDS

The legal relevance of standards can be 'explicit' where they are referred to in binding legislative or regulatory measures.[95] This can be done to facilitate adherence with the law and to support the obligations imposed by law, i.e. standards can be used as a tool of

[93] Although the ISO/IEC standard is likely to emerge soon.
[94] Lessig, L., *Code and other laws of cyberspace*, Basic Books, 1999.
[95] Kees Stuurman 'Legal Aspects of Standardization of Information Technology and Telecommunications: An Overview' [1992] 8 *CLSR* 2-10, at 4 for discussion of legal relevance.

compliance.[96] Standards are not generally binding, their application being a voluntary decision for the business. Nevertheless, the use of standards by legislators to support legislation is common for international standards[97] and is encouraged in many jurisdictions.[98] Another means by which standards can obtain public law effect is where an entity's ostensible adoption of a standard is held to be a deceptive trade practice.[99] Here, while adoption remains voluntary, the business may be held to account if its practices are at substantial variance from its declaration of adoption, such as to be considered misleading.

At the European level, the EU makes wide use of the option of referencing standards in legislation.[100] This incorporates both direct and indirect reference to standards. Direct reference to standards means that a specific standard is directly quoted within a legal text and consequently is made mandatory and part of the legislative act. A more flexible approach is to include indirect references to standards, as used in EU standardisation based on the New Approach[101] under which the European Commission can request the European standards organisations (ESOs)[102] to develop harmonised European standards necessary to comply with the 'essential requirements'[103] defined in the legislation. Standards remain voluntary but compliance with them provides a presumption of conformity with the essential requirements set out in the legislation.

To date, there is no European legislation directly referencing any cloud standards. In addition, the Commission has not requested any of the ESOs to develop standards for cloud computing, instead tasking ETSI only with 'mapping' the relevant standards and identifying gaps.

Furthermore, referencing standards in legislation is a step towards regulation and could have unforeseen and unpredictable consequences in an immature market. Although the Commission in its strategy communication on cloud[104] expressed concern about the lack of interoperability between cloud providers, for example, it does not suggest that cloud operators should be forced to interoperate.[105] Similarly, it does not propose that data

[96] Moore, R., 'Standardisation: A tool for addressing market failure within the software industry' *Computer Law & Security Review* 29 (2013) 413-429, discusses how the ISO/IEC 2007 series of information security standards is recognised by court and regulators.
[97] International Organization for Standardization, *Using and Referencing ISO and IEC Standards for Technical Regulation*, September 2007.
[98] E.g. National Institute of Standards and Technology, *NIST Report on the Use of Voluntary Standards in Support of Regulation in the United States* (October 2009).
[99] E.g. in the US the Federal Trade Commission can bring enforcement action against companies for "unfair or deceptive acts or practices" (15 U.S.C. § 45(a)(1)).
[100] For examples of how this has been used in the EU, see European Commission *Methods of referencing standards in legislation with an emphasis on European legislation* (2002, Enterprise Publications European Commission).
[101] Directive 98/34/EC of the European Parliament and Council of 22 June 1998 procedure for provision of information in the field of technical standards and regulations and rules on Information Society services (OJ L204, 21.7.1998).
[102] The European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and ETSI.
[103] These reflect the derogations expressly provided for in the TFEU, i.e. "on grounds of public policy, public security or public health" (Article 46), and recognised in ECJ jurisprudence, e.g. Case C-18/88, *Régie des Télégraphes et des Téléphones v GB-Inno-BM SA* [1991] ECR I-5941.
[104] Commission Communication.
[105] Although the Commission has the power to mandate interoperability in certain circumstances, for example, it has powers to mandate access to infrastructure under general competition law in relation to dominant firms under Article 102 TFEU. See Section on Refusal to Supply in Whish and Bailey, *Competition Law* (OUP 2012, 7th ed.) 697-709. It also has this power under sector-specific legislation

portability should become a legal right for cloud users. Even if there were agreed-upon industry standards on interoperability or data portability, it does not propose to reference these standards in EU legislation. Therefore, the legal effect of any cloud standard, even if supported by the main international standards organisations, is likely, for the moment, to be entirely based on industry accepting and adopting the standard and with enforcement based on private law (discussed below). Nevertheless, referencing standards in EU legislation remains an option for the European Commission in the event that the market develops in such a way that voluntary industry-based regulation is inadequate to deal with competition or other problems arising from lack of standards.

4.2 PRIVATE LAW AND CLOUD STANDARDS

When a cloud provider 'adopts' a standard, the provider can be viewed as making a unilateral statement to the world about its future conduct. Such statements may be considered to have contractual and tortious significance, as a unilateral contract[106] or a representation upon which others rely.

4.2.1 STANDARDS AND CONTRACTUAL LIABILITY

The most common way in which standards can have legal effect in private law is through contract. Contracts between private parties sometimes refer to standards and can require conformity to particular standards, failure to conform with which could then be actionable as a breach of contract.

In drafting a contract, the parties may refer to official standards, or *de facto* standards or even draft standards if no official standard exists at the date of the contract.[107] The use of official standards has the advantage that the content of the standard is fully described in the relevant standards document. This also makes it easier to enforce if the parties bring a contractual dispute to court. That said, if the parties define the *de facto* or draft standard in enough detail in the contract, this should avoid disagreements between the parties as to the standard to be achieved and be clear enough for a court to interpret whether or not one of the parties is in breach of its contractual obligations. In the case of cloud computing contracts, standards are generally detailed in an SLA or attached schedules.

Stuurman raises the question of whether reliance on a relevant standard can have effect in a contract where there is no explicit reference to the standard.[108] This could occur when the contract requires that one of the parties achieve a particular level of performance or quality or security but has not made reference explicitly to a particular standard. The question is under what circumstances a standard (official or *de facto*) can be assumed to influence the obligations of the contracting party and can be relied on in court as evidence of failure to fulfil contractual obligations. He argues that where the parties intended to rely on a higher level of quality or security than an industry standard, then the substance of this would need to be stated explicitly.[109] Nevertheless, Stuurman leaves open the question of whether, in certain circumstances, a court could interpret failure to adhere to an official standard as a breach of the implied terms of the contract. It

---

relating to the new liberalised network industries. For an example, in relation to telecommunications, see Chapter 8 on Access and Interconnection in Ian Walden *Telecommunications Law and Regulation* (OUP 2012, 4th ed.).

[106] *Carlill v Carbolic Smoke Ball Co* [1893] 1 Q.B. 256.

[107] Stuurman, p. 6 'Standards and Contractual liability'.

[108] Stuurman, p. 6

[109] Stuurman, p. 6

is not uncommon for contracts to require performance to at least industry standards, or industry best practice, or some similarly open-ended term. If it can be shown, as a matter of fact, that most industry players adhere to a particular standard, failure to do so would be evidence in support of a finding of breach.

In the case of cloud contracts, imposing adherence to an 'official' standard as an implied term would appear to be a big step for a court to take. Consequently, explicit reference to a cloud standard in the contract appears to be the most plausible way in which that standard could have legally-binding force in respect of contracting parties.

4.2.2 STANDARDS AND TORT LIABILITY

Standards may also be invoked in tort cases, particularly evaluative standards. A tort is distinguished from a breach of a contract in that a tort is a violation of a duty established by law, whether in common law or statute, whereas a breach of contract results from a failure to meet an obligation created by the agreement of the parties.

Official standards could be recognised by a court in tort law as a standard of conduct or care necessary to be met by the defendant. However, the relevance of the standard would depend on the duty of care established by law.[110] Compliance with a standard, even where specified in a regulatory instrument, will not automatically mean that the required level of care has been exercised, since it may be held that the standard was below that considered appropriate in the circumstances.[111] Equally, non-compliance with a standard may not impose liability depending on the extent of the duty of care. Therefore the extent to which a standard would be relevant in tort cases would vary greatly.

In the case of cloud standards, this will imply that standards have to have a minimum level of acceptance within the industry before they can become the 'standard of care'. A standard adopted by a minority of cloud providers may not be enough to convince a court that this is established as what a cloud user should expect from its provider. Nevertheless, as cloud standards are adopted, if it transpires that compliance with a certain standard or standards is considered 'normal industry practice' for certain cloud operations, this may sway a court and, perhaps, at least develop a minimum standard of care to be applied. To date, it is too early to point to any potential cloud standards that could be considered as equivalent to the 'standard of care' for tort liability.

In the case of cloud standards, pointing out that the provider has adhered to official standards may provide a defence to any claim. This may be particularly relevant for cloud contract terms relating to data protection or security, where it may be impossible to prove that the data have been secure. If the cloud provider can show adherence to an industry standard, and thus that reasonable measures have been taken,[112] he may escape tort liability if, despite his actions, there is a data or security breach.

---

[110] See Moore, p 427 for a discussion of difficulties in relying on standards in tort cases on software liability.

[111] See *Baker v Quantum Clothing Group* [2011] UKSC 17, where Lord Dyson noted that a standard in a code of practice or regulatory instrument may be compromised for various reasons, including a failure to reflect the latest technology, thereby rendering it no longer effective as a defence to a claim in negligence (para. 101). In the US, see *In re Eastern Transportation Co. (The TJ Hooper)* 60 F.2d 737 (1932).

[112] See Data Protection Directive, at art. 23(2).

4.3 LEGAL EFFECT OF CERTIFICATION FOR CLOUD STANDARDS

Certification is often used to demonstrate compliance with a standard. A certification scheme can be defined as the collection of requirements, procedures and means available for obtaining a certificate.[113] It has been defined as 'the successful conclusion of a procedure to evaluate whether or not an activity actually meets a set of requirements'.[114] Certification is often the final stage of a longer process, usually called 'conformity assessment', during which a person or body will evaluate compliance of persons, products and/or processes with a given set of requirements.[115] In relation to evaluative standards, which indicate that certain levels of quality or security have been met, a certification process offers an objective third-party assessment of compliance, which further generates trust among customers that the service attains the required standard.

Certification schemes can cover people,[116] products or organisations.[117] Certification can be provided by the entity itself or by an external organisation. In first-party certification or 'self-certification', the provider of the good or service 'self-certifies' by offering a public assurance that it meets certain standards. Third-party certification involves an independent assessment declaring that the requirements for certification have been met. Accreditation is the formal recognition by an independent body, generally known as an accreditation body, that a certification body is capable of carrying out certification, i.e. has the requisite expertise to make the assessment. Accreditation may not be obligatory but it provides an independent confirmation of the certification body's competence. In the EU, each Member State is required to have one national accreditation body that can provide an authoritative statement of the competence of any particular certifier to perform conformity assessment activities.[118]

Obtaining certification will usually be a voluntary choice of a company, so it does not necessarily indicate that a certified company is more compliant with standards than an uncertified company.[119] Nevertheless, despite the voluntary nature of certification to a particular standard, certification can still have legal consequences, namely a presumption, albeit one that is rebuttable, of conformity with the law arising from certification.[120]

---

[113] ENISA, *Security certification in practice in the EU* (October 2013), 6 ('ENISA 2013').
[114] Casper, C., & Esterle, A., *Information Security Certification: A Primer: People, Products, Processes*, (ENISA, December 2007) 2.
[115] ENISA 2013.
[116] For example, certification of expertise after a training programme.
[117] For organisations, it is important to note that a certification may be limited to a particular sector of its activities or for specific applications.
[118] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of product and repealing Regulation (EEC) No 339/93, L218/30, 13.08.2008
[119] Certification presents a problem of adverse selection in that where there is information asymmetry, less trustworthy companies want to use certification to appear as trustworthy companies. Herschel l. Grossman, 'Adverse Selection, Dissembling and Competitive Equilibrium' *The Bell Journal of Economics*, Vol. 10, No.1 (Spring, 1979) pp 336-343.
[120] The legislative mechanism giving a presumption of legality with certification to European standards is a feature of the New Approach Directive in the EU. This approach means that compliance with the standard remains voluntary – there is no legal obligation in the Directives to comply with any standard – but certification to the standard carries a presumption that the product is in conformity with the essential requirements of the Directive. Lack of certification does not confer a presumption of illegality, but the manufacturer is required to demonstrate by other means that his product conforms with the relevant Directive.

From a legal perspective, self-certification may not give rise to any private law rights between the 'self-certifier' and its customers or those who have relied on its certification. Nevertheless, it may lend support to claims by its customers if in fact it can be demonstrated that it did not conform to a particular standard.

However, if the self-certification were supported by contractual guarantees that the company has achieved and will maintain that certification, this would give reassurance of compliance to those contracting with the provider. The backing of self-certification by contractual guarantees in SLAs is suggested by ENISA as a way of giving more satisfactory assurance of compliance.[121]

One issue with certification is that the acceptance of certification internationally is unclear and there is no automatic mutual recognition of certification schemes. This in itself could be a barrier to cloud take-up with multiple certifications needed in different regions or, indeed, different accreditation bodies depending on the acceptance of certification in one region or another. This is an issue even within the EU. A problem identified by ENISA[122] is that many EU Member States have different sets of security requirements for the procurement of IT and, therefore, certification under one scheme does not imply compliance with security requirements in another Member States which increases the problem of mutual recognition of certification.[123]

5. CONCLUSION

As we have seen, a proliferation of standards is not necessarily symptomatic of a problem for the cloud industry, being instead more a reflection of the variety and complex nature of the technologies that comprise the cloud ecosystem. Standards serve a multitude of different purposes, whether solving a technical problem; enabling interoperability; facilitating competition, or as a means of generating a trusted environment. The greater the degree to which a standard is developed to address, or becomes associated with, a public policy purpose (external), rather than an industry purpose (internal), the greater the likelihood that the standard will have legal effect, whether expressly sought or achieved through public or private law mechanisms.

The standards-making process will also generally differ between technical, informational and evaluative standards. The institutional structure within which technical standards are developed varies considerably from official to private, and formal to ad hoc arrangements; reflecting the diverse nature of the industry. By contrast, informational and evaluative standards will usually involve a broader range of stakeholder participants, either at the drafting stage or through consultation mechanisms designed to elicit input from interested or affected parties. Governance and accountability concerns are also more likely to arise in the development of informational and evaluative standards, reflecting their potential legal role.

To date, there does not appear to be a 'standards problem' in terms of interoperability, data or application portability that places cloud users in particular danger of being locked-in to their cloud provider. Many providers already allow data to be exported from their services in *de facto* standard formats. Work on technical standards for many aspects of the evolving cloud environment appears to be progressing in the manner

[121] ENISA 2013.
[122] ENISA, 9-10 'About the challenges: Two procurement scenarios'.
[123] W. Kuan Hon, Hörnle, J., and Millard, C., "Which Law(s) Apply to Personal Data in Clouds?" Chapter 9 in *Cloud Computing Law*, (ed. Millard) (OUP, 2013).

expected. A lack of standards in this area could be an issue as the cloud market develops but, for the moment, developments on cloud interoperability and data portability appear to be slow but uncontroversial.

There appears to be demand for informational and evaluative standards that reassure users about data security and data protection in the cloud, especially in the light of recent events, such as the Snowden revelations and the 'Heartbleed' vulnerability. It appears that all major standard-setting organisations, both public and private, are proceeding with initiatives in these areas. However, such standards need to reflect and take into account a multitude of legal frameworks that are themselves, just from an EU perspective alone, either undergoing fundamental reform or are the subject of new regulatory measures. As such, policy makers may be putting the proverbial 'cart-before-the-horse' by expecting rapid action on standards in such a complex and changing legal environment.