CHAPTER 9. Principles for regulating the cloud (2); based on the roles and functions across the cloud workflow

a. Introduction – scope of this chapter

Having examined the cloud down to its detail as technology and after proposing the regulatory principles that should be put in place to efficiently respond to the challenges posed by the technical particularities of it, it is now time to direct our attention to the way the cloud is perceived from the outside as an autonomous concept and an entity or environment which is defined by organic and functional self-sufficiency. In other words, our focus will now shift to the fact that, when a cloud computing network is understood as a workflow chart, it should be at any time possible to point down the entry and exit point in it, to define the distinct functions performed in order for the entire workflow to produce the expected end-product and, respectively, to recognize the duties, obligations and expectations anchored to every such function and, consequently, to the actor (or actors) performing it.

Reference has already been made, in earlier parts of this study[954], to the issue of the internal vs. external perspective in law and how this is all the more crucial when it comes to internet law and cloud computing, in particular. In light of this theorem, and having already explored the cloud in an analytical manner with regard to its 'inner nature' as a technology and technical arrangement – an aspect of it that could be described as its internal dimension with regard to laws governing it – it is now time to research into the question of what constitutes the external aspect of cloud computing and whether we can pinpoint further regulatory principles for it stemming from that perspective of looking into cloud computing.

But first and foremost, it is necessary to look into the question of whether the cloud does have an external, apart from an internal aspect and what it constitutes of.

---

954 See Chapters 4 and 5.

b. Viewing cloud computing from the outside; what else is the cloud apart from its infrastructure and the science behind it?

One of the most discussed legal notions in recent years is that of the internal versus the external perspective of law[955]. The concept has become of particular importance and is gaining more and more in prominence as legal subject matters become of a continuously more complex nature, with multiple levels of reference and substance that does not stem only from themselves but also through extrapolation to other notions or phenomena that interact with them, one way or another[956]. Simultaneously, this internal vs. external structure refers to the two distinct ways in which a regulatory subject matter can be observed and, consequently, analyzed and regulated[957]. Actually, this aspect of the topic applies to even more legal phenomena, not only modern but also more traditional ones. It refers to rules that are developed to regulate a phenomenon just by observing the phenomenon itself as opposed to rules which are developed in order to settle regulatory issues arising from the interaction of the said phenomenon with other subject matters or actors external to it[958].

Focusing on the realm of the internet, and bearing in mind that a regulator's main challenge is to create rules that will be clear enough to allow the lawyer and law subjects, in general, to simply apply legal provisions to facts, a difficult question pops up: "what are the 'facts' when it comes to the world of the internet and IT?"[959]

The facts of anything related to the Internet depend on whether you look for them focusing on physical or virtual reality[960]. From the angle of virtual reality, we view the Internet from the perspective of a user who understands the virtual world of cyberspace and the actions and processes happening there as an analogy to the equivalent instances in the offline, physical world. Alternatively, we can perceive internet facts based on the physical reality of how the network operates. From this angle, Internet

955 Orin S. Kerr (note 230).
956 Trevor Bench-Capon & Giovanni Sartor, *A model of legal reasoning with cases incorporating theories and values*. *AI and Law*, 150 Artificial Intelligence 97–143 (2003.)
957 Orin S. Kerr (note 230).
958 *Id.*
959 Urs Gasser, Cloud Innovation and the Law: Issues, Approaches, and Interplay (2014.)
960 L. Lessig (note 504).

transactions are interpreted based on how the network actually works "behind the scenes" and on the inside, irrespective of the perceptions of a user[961]. When it comes to cloud computing, so far, we have been producing laws which primarily focus on the external perspective and are developed to provide answers to the regulatory challenges we perceive when observing the cloud through the applications that are made possible thanks to it. However, as it has already been demonstrated in the previous chapter[962], we still miss critical aspects of the cloud which remain unregulated and which we can only understand if we observe the cloud from the inside, i.e. from the perspective of an entity that is participating itself to a cloud network's workflow or from the angle of an observer who focuses on each of these distinct entities and the role(s) they play across the life cycle of a cloud network regardless of what the external manifestation of their function(s) may be. We have already executed this internal observation in the previous chapter, where the cloud was analyzed as far as its infrastructural element is concerned. However, in order to have the complete picture of the cloud's internal world, it is imperative to examine it also from the aspect of how the life cycle developed around this infrastructure looks like, how it works, what processes it is made of and which actors and with which roles take part in those processes. After all, we should not forget that the final manifestations of the cloud, i.e. the end cloud based applications that reach end users, need a facilitating background to be hosted in, which should not escape our attention as to the regulatory issues that may arise within it. Last but not least, this enabling background corresponds to the internal aspect of a work line which aims at making available the various cloud based applications to the market, i.e. to their pool of intended users, regardless of whether they pay a fee to make use of them (as it is usually the case) or not.

There have already been scholars who have attempted to view the realm of the Internet from this internal perspective[963]. Actually, Lawrence Lessig[964] has gone as far as attributing to code makers, such as Microsoft and AOL, qualities of 'virtual governments that exercise real control over the virtual world of cyberspace' suggesting that we should consider subjecting their decisions not just to plain legal but to constitutional scrutiny.

---

961 *Id.*
962 See Chapter 8.
963 Bibliographical index (or internal reference.)
964 Lawrence Lessig (note 505).

It is quite revealing to examine the famous theory of Lessig arguing that "code is law"[965] through this internal vs. external perspective lens. In fact, the very phrase "code is law" reveals a relationship between the internal and external perspectives. In detail, on the software front "code is law" extrapolated through the internal vs. external perspective prism means that what is perceived as code from the external perspective has the gravitas of law from the internal one. A software program's code stipulates the architecture of the virtual world that a user encounters while making use of that program. Consequently, as external code is internal law, we need to regulate not just the manifestations of this program in the external world but also its functioning from an internal perspective. Mutatis mutandis, in the case of cloud networks, for a complete regulatory framework to be put together we need to regulate not just what users are confronted with as the external manifestation of the cloud processing done for them to receive the end applications they have asked for but also the processing itself as it happens on the inside of the network, as well as the different stages through which the processing passes and the agents that push it forward at each one of these stages.

Viewing Lessig's theory through this internal vs. external perspective prism helps us also understand how he went as far as proposing the application of constitutional norms in cyberspace[966]. Lessig has probably been the most tenacious scholar to date suggesting that the Internet should be directly subject to constitutional norms from an internal perspective. He has actually found it is high time to apply rules of constitutional gravity to the world the Internet user perceives, just as we do to the offline world. In order to determine who is subject to which constitutional norm in the Internet realm, Lessig proposed the paradigm of state actor as our guide. We can determine who is a state actor online, according to Lessig[967], by looking at the online world from an Internet user's perspective and determining who has powers that resemble those of the government. In this way, Lessig suggests, we will be able to transpose constitutional values to cyberspace just by recognizing the user's perception of the online world as the functional equivalent of the physical world. With regard to cloud computing, it is not necessary to go as far as constructing such an exhaustive hierarchical order for laws applicable to everything related to the cloud.

965 L. Lessig (note 504).
966 Lawrence Lessig (note 505).
967 *Id.*

As a first step, it would already make a substantial difference to recognize the difference between the external manifestations of the cloud and its internal aspects and deal with the need to concretize rules that will regulate the latter. **The relationship between these two pools of laws (i.e. the already existing and abundant one of laws regulating cloud-based applications and the currently nascent or almost non-existent but needed one of rules regulating the cloud per se) is not hierarchical but rather complimentary: enriching the latter will further boost the efficiency of the former.**

The prism of perspective for dealing with and regulating the cloud proves that rules specifically constructed for cloud computing do add up something new to the broader sector of internet law — not so much with respect to how we approach the law, but more in the way that we approach the facts surrounding the cloud. Modeling the reality of cloud computing reveals that this is not as simplified as we have been thinking so far, and that we need to look into both dimensions of the cloud, the internal and the external one, in order to get the whole picture.

The dual perspective through which it is either possible or necessary to view all sorts of systems that make information and data exchange possible is not anything new[968]. Actually, the first instance in which the internal and external perspectives competed with each other demonstrating that they both exist and that they are both essential in understanding and regulating communication enabling systems is the famous telephone wiretapping case of Olmstead v. United States of 1928[969]. In summary, that case dealt with government agents who had wiretapped the telephone lines of a former police officer who operated a bootlegging operation in violation of the Alcohol Prohibition laws. The authorities tapped the phone lines from a city street without entering the plaintiff's private property. At first and second degree, Olmstead argued that the wiretapping had violated his Fourth Amendment rights. The Justices' opinions are demonstrative of how decisive the adoption of either the external or the internal perspective was already since that time for adjudicating (and regulating) on issues and phenomena of the wider data and communications realm. Writing for a 5-4

968 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stanford Law Review 247–316 (2011.)

969 Olmstead et al. v. United States; Green et al. v. United States; McInnis v. United States, 277 U.S. 438, 43 S. Ct. 394; 67 L. Ed. 785; 1923 U.S. LEXIS 2588; 24 A.L.R. 1238.

majority, Chief Justice Taft rejected Olmstead's argument following a reasoning tantamount to an external comprehension of the telephone network. According to Taft, "the telephone network consisted of electrical lines that permitted its users to send communications out into the world. By using a telephone Olmstead and his co-conspirators had opted to send their communications out from the protected spaces of their houses and into the unprotected space of the public city street"[970].

In contrast, Justice Brandeis's dissenting opinion portrayed an internally comprehended account of the same event. In Brandeis' opinion[971], it was "immaterial where the physical connection with the telephone wires leading into the defendants' premises was made." Rather, "the proper question was whether from a telephone user's perspective, the wiretapping appeared as the equivalent of a search and seizure". Brandeis thought that it appeared so: "Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard."

Of course, what Justice Brandeis described does not entirely amount to Lessig's internal perspective of cyberspace or the herewith suggested internal aspect of cloud computing; however, it is interesting to note how close he came: Brandeis, in a pioneering manner, understood telephony not just as a service but, in addition to it, as infrastructure; in fact, he conceived the telephone network as the technological means of creating a private space for its users. Already almost a century before, the divide between Taft and Brandeis was not so much a contest between dogmatic and dynamic interpretation of laws, as it was a clash of perspectives for interpreting the facts of the case. Taft applied an external perspective of the telephone network, while Brandeis used an internal one.

Needless to say, this case was only a primary forerunner to the whole issue of the internal vs. external perspective and the great importance these two have today with regard to regulation of the internet, as a whole, or cloud computing, more precisely. Given that the telephone simply transmits sound from one place to another, its ability to generate a virtual reality is very limited. Consequently, telephone cases with an internal-external dynamic have been rare through all previous decades since the in-

970 Id.
971 Id.

vention of telephony, and considered as a whole, they cannot account for a recurring problem of perspective. Things are fundamentally different though, when we focus on the most modern technologies facilitating communication today through the transmission and exchange of all kinds of data and not just sounds[972]. The advanced technology of the Internet has elevated to a universal level a problem that remained largely marginal in the early steps of the telephone network. Some could use the opportunity to cast in doubt whether the problem of perspective is truly "new". This is, however, of little importance. What truly matters is that, one way or another, the problem recurs more and more in Internet law, challenging us to confront it across a wide range of substantive areas[973]. What is more, while in some sub-sectors of IT law effective regulation is achievable only by choosing to focus on one of the two perspectives, when it comes to regulating cloud computing, it is not a matter of choice anymore; rather, it is of vital importance to look into the issues raised by both perspectives and come up with rules that will deal with all of them in order to end up with an all-inclusive range of regulations that will manage to persuasively answer to all challenges posed by the cloud.

c. Completing the picture of the inner side of the cloud; regulatory challenges stemming from the cloud network's business workflow

It has by now been established that, in order to end up having a complete set of rules that will be dealing with cloud regulation in a holistic manner, it is imperative to look into all aspects of the internal side of cloud computing. According to extensive literature[974], the internal perspective of the cloud also includes, apart from what pertains to its infrastructure and raw

---

972 M. Armbrust, A. Fox, R. Griffith, A. Joseph D., R. Katz H., A. Konwinski, G. Lee, D. Patterson A., A. Rabkin, A. Stoica & M. Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, available at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html (2 March 2015.)

973 Colin J. Bennett & Charles D. Raab, The governance of privacy. Policy instruments in global perspective (2006.)

974 For a comprehensive review of what the cloud and cloud networks actually consist of as technical arrangements, refer to: Ines Houidi, Marouen Mechtri, Wajdi Louati & Djamal Zeghlache, *Cloud Service Delivery across Multiple Cloud Platforms*, in 2011 IEEE International Conference on Services Computing, 741–742 (IEEE Staff ed., 2011); Hoang T. Dinh, Chonho Lee, Dusit Niyato & Ping Wang,

machinery, all structures, workflows and the organizational scheme under which the entire cloud network is set in motion and operates. These workflows could be more easily understood as the organigram of the cloud network, consisting of the actors taking part in it and the functions each of them is performing. What is more, our attention will now move on the service composition methods[975], namely aggregation[976], customization[977] or

---

A survey of mobile cloud computing. *Architecture, applications, and approaches*, 13 Wirel. Commun. Mob. Comput. 1587–1611 (2013); Thomas Erl, Richardo Puttini & Zaigham Mahmood (note 46); Liang-Jie Zhang & Qun Zhou (note 96); Won Kim, *Cloud computing architecture*, 9 IJWGS 287–303 (2013); Wei-Tek Tsai, Xin Sun & Janaka Balasooriya, *Service-Oriented Cloud Computing Architecture*, in ITNG 2010. Information Technology New Generations : proceedings of the Seventh International Conference on Information Technology :12-14, April 2009, Las Vegas, Nevada, USA, 684–689 (Jameela Al-Jaroodi & Shahram Latifi eds., 2010); Yashpalsinh Jadeja & Kirit Modi, *Cloud computing – concepts, architecture and challenges*, in 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 877–880 (2012); Bu-Qing Cao, Bing Li & Qi-Ming Xia, *A Service-Oriented Qos-Assured and Multi-Agent Cloud Computing Architecture*, in Cloud computing. First international conference, CloudCom 2009, Beijing, China, December 1-4, 2009 : proceedings, 644–649 (Martin Gilje Jaatun, Gansen Zhao & Chunming Rong eds., 2009); Liang-Jie Zhang & Qun Zhou (note 96); Christian Baun, Marcel Kunze, Jens Nimis & Stefan Tai, Cloud Computing (2011); Vijay Sarathy, Purnendu Narayan & Rao Mikkilineni, *Next Generation Cloud Computing Architecture: Enabling Real-Time Dynamism for Shared Distributed Physical Infrastructure*, in 2010 19th IEEE International Workshop on Enabling Technologies. Infrastructures for Collaborative Enterprises, 48–53 (IEEE ed., 2010.)

975 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar, *The Business Perspective of Cloud Computing: Actors, Roles and Value Networks* ECIS 2010 Proceedings (2010). For more on service composition in cloud computing, refer to: Amin Jula, Elankovan Sundararajan & Zalinda Othman, *Cloud computing service composition*. *A systematic literature review*, 41 Expert Systems with Applications 3809–3824 (2014); Cheng Zeng, Xiao Guo, Weijie Ou & Dong Han, *Cloud Computing Service Composition and Search Based on Semantic*, in Cloud computing. First international conference, CloudCom 2009, Beijing, China, December 1-4, 2009 : proceedings, 290–300 (Martin Gilje Jaatun, Gansen Zhao & Chunming Rong eds., 2009.)

976 See also Chapter 7.

977 For further details on the margins for customization on cloud computing networks refer to: Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg & Ivona Brandic, *Cloud computing and emerging IT platforms*. *Vision, hype, and reality for delivering computing as the 5th utility*, 25 Future Generation Computer Systems 599–616 (2009); Tharam Dillon, Chen Wu & Elizabeth

service distribution channels[978], and what kind of dynamics and interrelations these processes develop, which may lead consequently to corresponding regulatory challenges that need to be dealt with. It needs to be pointed out right from the beginning that, although the following arguments will primarily be presented in light of the way cloud networks aimed at facilitating commercial applications of the cloud are built, the observations and recommendations made here largely fit also with those cloud networks deployed for the provision of hybrid or private services[979].

It is a very well-established practice in the industry[980] to classify cloud services along different layers; and we have already seen a most detailed and representative such listing[981]. Various cloud services fall all in one of the five layers of this ontology, which represent a level of abstraction, permitting the user to set aside all underlying or higher-ranking components and thus providing simplified focus to the resources or functionality that correspond to each one of them. However, the actors and entities making all these services possible can be spotted in more than one layers of the overall ontology[982]. At the same time, one entity that can occupy the position of one specific (and with particular tasks) actor on one layer can simultaneously occupy the position and responsibilities of a different actor on another layer[983].

Chang, *Cloud Computing: Issues and Challenges*, in 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2010. 20 – 23 April 2010, Perth, Australia; proceedings, 27–33 (Elizabeth Chang ed., 2010); Lamia Youseff, Maria Butrico & Dilma Da Silva (note 838); Wei-Tek Tsai, Xin Sun & Janaka Balasooriya (note 974).

978 For a broader review on the issue of service distribution channels on cloud networks refer to: Kaiqi Xiong & Harry Perros, *Service Performance and Analysis in Cloud Computing*, in World Conference on Services-I, 2009, 693–700 (Liang-Jie Zhang ed., 2009); Thomas Erl, Richardo Puttini & Zaigham Mahmood (note 46); M. Armbrust, A. Fox, R. Griffith, A. Joseph D., R. Katz H., A. Konwinski, G. Lee, D. Patterson A., A. Rabkin, A. Stoica & M. Zaharia (note 972); Hoang T. Dinh, Chonho Lee, Dusit Niyato & Ping Wang (note 974).

979 Kristina Irion (note 220).

980 Cong Wang, Qian Wang, Kui Ren & Wenjing Lou (note 932).; Lamia Youseff, Maria Butrico & Dilma Da Silva (note 838).; Benoit Dupont (note 111).

981 See Chapter 2.

982 Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang & Anand Ghalsasi (note 116).

983 *Id.*

With these in mind, it becomes clear that in order to single out the regulatory challenges posed by the workflow on which cloud networks typically run today a detailed review of the actors present throughout these networks and their typical roles is required. It needs to be made clear that the actors that will be analyzed hereunder can be present and found on many different layers of the cloud network ontology. Therefore, their order of presentation is random and does not imply any hierarchical or significance sequencing among them:

i. The customer[984] (or user) of cloud computing services

It is the actor who, through various distribution channels buys and makes use of the different cloud services commercialized by the provider[985]. The channels through which the customer can finally receive the services of his choice can be various, namely directly from the service provider or through a platform provider or through a reseller[986]. It needs to be stressed out that a customer of a cloud service can be found on all layers of the cloud ontology. One of the most characteristic elements of customers of cloud services is the ways in which they interact with the service itself, with only rare exceptions to the rule given that, even those that may also have physical access to the infrastructure facilitating the service they use some kind of tool or intermediary facility to interact with the resources of that infrastructure[987]. In particular, users access cloud computing to enjoy the services of their choice using networked client devices, such as desktop computers, laptops, tablets and smartphones, but also practically any Ethernet enabled device. As time goes by, several of these devices turn into actual cloud clients, as they rely more and more exclusively on cloud computing in order to execute all or the majority of their applications being rendered essentially useless without it[988]. As it becomes evident, it

984 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar (note 975).
985 *Id.*
986 Stephanos Androutsellis-Theotokis & Diomidis Spinellis (note 861).; Lothar Determann, *What Happens in the Cloud: Software as a Service and Copyrights*, 29 Berkeley Technology Law Journal 1096–1129 (2015.)
987 Mike P. Papazoglou & Willem-Jan van den Heuvel (note 853).
988 *Id.*; J. Hoover, *Compliance in the Ether: Cloud Computing, Data Security and Business Regulation*, 8 Journal of Business & Technology Law 255–273 (2013.)

would be unrealistic to go as far as standardizing these devices with which users get access to the cloud; that would be a totally unfounded intervention to the market of these products[989]. Therefore, the need for defining minimum requirements that these devices should satisfy emerges so that cloud customers can expect and actually get a minimum quality of access to the network no matter what medium they choose to enter it with. Some would argue that the solution to this need would be for regulators to define the minimum specifications of the pieces of hardware used to facilitate access to the cloud. However, it makes much more sense to define the minimum conditions (in terms of security etc.) that access to the cloud should have than trying to homogenize the range of devices suitable for it. This approach makes even more sense if we bear in mind that many cloud applications do not require some sort of specific software on the client from which they are accessed[990]; instead, a web browser to interact with the cloud application would suffice. Apart from this main path for users to access the cloud, there is a smaller group of customers who make use of highly niche services[991] which necessitate the use of specific client software dedicated to them (for instance, virtual desktop clients and most email clients). At last, there is a pool of customers[992] who use a number of legacy cloud applications (mostly from the front of business applications) that are delivered via a screen-sharing technology. All of the above strengthen the argument that we need rules that will mandate the minimum conditions under which customers will have access to cloud networks and the services they wish to use through them, since regulating how the means of access should look like would be too complicated and an unnecessarily interventionist route. If customers are assured, thanks to clear and established rules, that any of the lawfully commercialized cloud services on the market meets the minimum requirements guaranteeing safe and unequivocal access to it, then it is only logical that customer safety and trust will increase, opening up simultaneously the way for providers to freely antagonize for anything superior to those minimum standards maintaining

989 Benoit Dupont (note 111).
990 Christof Weinhardt, Arun Anandasivam, Benjamin Blau, Nikolay Borissov, Thomas Meinl, Wibke Michalk & Jochen Stößer (note 65).
991 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar (note 975).
992 *Id.*

a level of market competition that can only prove further beneficial to customers.

ii. The service provider[993]

It often also called IT vendor, is the actor within a cloud network typically executing development and operation of services that offer value to either the customer or the aggregate services provider. Service providers, within the range of their functions, develop applications that are offered and deployed on the cloud computing platform and, to this end, access hardware and infrastructure contributed to the network by the infrastructure providers[994]. Bearing in mind the above definition, we can now analyze the specificities of the role of service provider and the respective regulatory challenges that come along with them;

– Firstly, it is essential to point out that, despite the fact that a service provider can also function as a customer within the flow of a cloud network, this happens only in relation to hardware resources which are necessary for the deployment of the services addressed to cloud customers or aggregators[995]; this kind of buys (i.e. referring exclusively to hardware) are already sufficiently and effectively regulated by existing commercial transactions laws and they should not be equated to the observations made above regarding the functions of the cloud computing customer.
– One of the most important tools in the hands of service providers on the cloud is monitoring performance[996] of their services and the network's resources in order to do any tweaking or other interventions necessary for the performance index to remain or reach optimal levels. In conducting these performance measurements service providers need to be forced by law not to compromise core features that their services are supposed to offer to cloud customers, namely privacy of users' data, protection of their identity etc.

---

993 Siani Pearson & Nick Wainwright (note 645).
994 M. Armbrust, A. Fox, R. Griffith, A. Joseph D., R. Katz H., A. Konwinski, G. Lee, D. Patterson A., A. Rabkin, A. Stoica & M. Zaharia (note 972).
995 Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang & Anand Ghalsasi (note 116).
996 Lothar Determann (note 986).

– Security is one of the competitive advantages that boosted cloud computing to the absolute standard technology of today's internet and data networks[997]. As it has already been analyzed, security on the cloud is improved in comparison to older technologies due to a number of factors, such as centralization of data, increased security-focused resources, etc[998]. Nevertheless, there are still unsettled issues concerning the security of core cloud services such as the ones made available by service providers. The main points of concern over security on the cloud on the service providers level are uncertainty over the possibility of loss of control over certain types of sensitive data, or the lack of security for stored kernels[999]. What improves security on the cloud over older, traditional systems is its capacity to devote resources to solving security issues (on a proactive or a posteriori basis) in a magnitude and volume that many customers cannot afford to by themselves or which they do not possess the technical skills to address[1000]. Rules are, therefore, necessary that will force service providers to deploy these security optimization techniques on a standard basis and not just as a competitive advantage. At the same time, security on the cloud becomes an all the more complex idea when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users[1001]. Additionally, user access to security audit logs may be difficult or impossible as the expanse and complexity of the cloud network increases. Therefore, regulators need to strike a balance between the conflicting interests of security and optimization of the cloud networks economies of scale (which is the main drive behind the increasing vastness and confluence of totally estranged streams of data over the same network[1002].
– The above points of concern exist in the cases of public and hybrid clouds. In private clouds, most of these issues are not applicable given that the infrastructure owner and the service provider are, as a rule, one and the same entity. However, it is not reasonable to claim that the an-

997 Siani Pearson & George Yee (note 280).
998 See Chapter 2.
999 See Chapter 8.
1000 Benoit Dupont (note 111).
1001 Kenneth A. Bamberger & Deirdre K. Mulligan (note 968).
1002 Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

swer to these security concerns would be the replacement of all public and hybrid cloud facilities by private ones given that this would financially unrealistic and would automatically compromise the cloud's most cherished element, i.e. the dynamics achieved due to virtualization. Between hybrid and public clouds, the former offer, in general better answers to the security concerns outlined above; however, at present and, likely, in general they cannot be the rule. Therefore, any rules established with a view to defining the minimum standards cloud networks should respect in light of the issues discussed with regard to service providers need to be designed with the case study of public clouds in mind.

– A key issue in relation to service providers in the cloud is the problem of legal ownership of the data[1003], which essentially translates to the question of whether the service provider can profit from users' data stored in the cloud. This issue will grow more and more in significance as the cloud penetrates the neighboring fields of big data and IoT, at the heart of which lie vast amounts of data originating from thousands of different users or entities[1004]. At the moment, most Terms of Service agreements remain silent on the question of ownership. The ideal answer would be, similarly to what has been argued before, the choice of network equipment upon which cloud customers would have immediate physical control over the computer equipment (private cloud); however, this is only rarely a choice. The present unregulated landscape with relation to legal ownership of data stored in the cloud creates great incentives to public cloud computing service providers to prioritize building and maintaining strong management of secure services. However, things will get all the more complicated as the big data and IoT applications multiply, given that in those cases the consent of data subjects regarding collection of data attributable to them is not always explicit nor can it be taken for granted[1005]. Moreover, as it widely the case, plain end users do not pay the necessary attention to service contracts, which is largely the case with regard to service agreements of most popular cloud services. The fact that for the time being the issue

1003 Hassan Takabi, James B. D. Joshi & Gail-Joon Ahn (note 119).; see also Chapter 6.

1004 Hunton Privacy Blog (note 269).; Viktor Mayer-Schönberger & Kenneth Cukier (note 321).

1005 *Id.*

of legal ownership of data remains unanswered does not necessarily mean that this will always be the case. As economic incentives will grow with the push from big data and IoT applications, service providers may very expectedly decide to deal with this question deliberately and in a manner not entirely balanced between theirs and the interests of their customers. Therefore, a clear answer to the issue on behalf of the law will only work to the benefit of customers, who are generally the inferior side in this equation. What is more, the sooner the issue is settled on behalf of cloud regulators the more balanced and fair the final settlement can be between the need of customers for non-exploitation of their data and the drive of service providers to maximize the profits they can derive from the data they host on their systems. Last but not least, looking at this issue now that big data and IoT have not yet reached their full capacity (although it is, of course, undeniable that they are on a steep rise) will permit cloud regulators to regulate on the matter of legal ownership with a clearer head and not under the pressure the whole topic may have in the near future, calling for immediate over proactive measures.

iii. Infrastructure providers[1006]

As actors of the cloud workflow, infrastructure providers are tasked with supplying the network with the computing and storage services needed in order for all subsequent software applications to run within the cloud. In other words, as we have already seen[1007], the infrastructure provider serves as the actor maintaining the technical backbone of the network. The resources offered by this actor are essentially scalable hardware for the services[1008] upon which the service providers offer their services. Infrastructure providers are alternatively called IT vendors. Typically, the consumer of what an infrastructure provider offers does not manage or control the underlying cloud infrastructure but retains control over operating systems, storage, and deployed applications, possibly even limited control of

1006 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar (note 975).

1007 See Chapter 2.

1008 Ozalp Babaoglu, M. Jelasity, Anne Marie Kermarrec, Alberto Montresor & Maarten van Steen (note 874).

select networking components (e.g., host firewalls). It becomes evident then, once again, at this point, that rules describing attribution and extend of responsibility and culpability between infrastructure providers and service providers (who are the customers of the former but providers to cloud applications customers) towards end users of the applications/services developed on a cloud network are crucial. In detail, the most basic cloud-service model[1009] is that where providers offer computing infrastructure – virtual machines and other resources – as a service to subscribers. It needs to be stressed out that Infrastructure as a service (IaaS), by today's state-of-the-art in the cloud business, refers to online services that set the user free from the details of infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. Those virtual machines, which are the vessels of most IaaS, are run by hypervisors[1010], i.e. companies that sit between the actual owners of the cloud network's infrastructure and the customers buying the right to use part of that infrastructure in the form of IaaS. This arrangement is yet one more argument in support of the need for developing rules that will clearly define how obligations and culpability are distributed among actors of the cloud workflow, particularly at this rudimentary level. In addition, it is common practice that hypervisors arrange themselves in pools within the cloud operational system in order to be able to support large numbers of virtual machines and to scale services up and down according to customers' varying requirements[1011]. The connection to the network's actual physical resources is then made possible via Linux containers[1012] running in isolated partitions of a single Linux kernel[1013] which connects them directly to the

1009 Xiaolong Jin & Jiming Liu (note 844).

1010 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar (note 975).

1011 M. Armbrust, A. Fox, R. Griffith, A. Joseph D., R. Katz H., A. Konwinski, G. Lee, D. Patterson A., A. Rabkin, A. Stoica & M. Zaharia (note 972).

1012 LXC (Linux Containers) are an operating system-level virtualization method for running multiple isolated Linux systems (containers) on a control host using a single Linux kernel. The Linux kernel provides the functionality that allows limitation and prioritization of resources (CPU, memory, block I/O, network, etc.) without the need for starting any virtual machines, and also namespace isolation functionality that allows complete isolation of an applications' view of the operating environment, including process trees, networking, user IDs and mounted file systems. (Definition cited as formulated under: https://linuxcontainers.org/lxc/introduction/; last accessed on 7/11/2016.)

1013 See also Chapter 8.

physical hardware. Containerization[1014] offers at this level better performance than virtualization, because there is no hypervisor overhead. Also, container capacity auto-scales dynamically with computing load, which eliminates the problem of over-provisioning and enables usage-based billing.

iv. Aggregate services providers (aggregators)

This is a niche sub-type of service provider that offers new services or solutions 'by combining pre-existing services or parts of services to form new services and offer them to customers'[1015]. As a result, aggregators are by nature a customer (from the perspective of the service provider) and a service provider (from the perspective of the customer). They can be further sub-divided into aggregators that focus on the integration of data and others that mostly offer aggregation of services with the former being quoted as data integrators[1016]. The main function of those is making sure that already existing data is prepared and is usable by different cloud services and can be regarded as a sub-role of aggregators with a primary focus on technical data integration. Similar types of cloud network actors are the "system integrator" or "business process integrator" or the "service mediator"[1017]. These terms describe, in general, aggregators that focus more on the technical aspects necessary for data and system integration while '(service) aggregators', as a generic term, also includes the business aspects of merging services to come up with new service bundles. The quasi-binary nature of aggregators stresses even more the need for cloud regulation rules that will permit allocation of responsibilities and culpability on each instance of cloud business workflow regardless of whether it

1014 Containerization is a lightweight alternative to full machine virtualization that involves encapsulating an application in a container with its own operating environment. This provides many of the benefits of loading an application onto a virtual machine, as the application can be run on any suitable physical machine without any worries about dependencies. (Definition cited under: http://www.webopedia.com/TERM/C/containerization.html; last accessed on 7/11/2016.)

1015 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar (note 975).

1016 Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang & Anand Ghalsasi (note 116).

1017 *Id.*

corresponds to an already known type of cloud service or a novel, still insufficiently charted one.

v. The platform provider[1018]

This is the actor that functions as the provider of an environment within which cloud applications can be deployed. We could place this actor on the same level as the kernel software that we have already seen in the context of the ontology of the cloud[1019]. Platform providers act as a kind of catalogue of reception in which different service providers offer services. Platform providers offer the technical basis for the marketplace where cloud services aimed at the end user are offered. It is very important to point out that platform providers can be hosted on the same development level and cloud space with the subsequent services they facilitate. However, it is also possible to have them located on totally different facilities as well. This raises serious issues of integrity of the data they handle as well as of the connections that bind them with the services nested in them, which points again towards the need for clear regulations referring to the inner side of cloud networks and the business cycles that are in full motion within them.

vi. The cloud services consultant

Lastly, the ever more complex structure of the cloud business has provided fertile ground to one more type of actor within the cloud business cycle, i.e. the **cloud services consultant**[1020]. Entities performing consulting for the customers on a cloud network serve as support for the selection and implementation by the latter of relevant services in order to create value for their business model[1021]. One might argue that the cloud consultant does not entirely fall within what we have described as the cloud network business workflow; nevertheless, those actors, in the context of assessing cloud customers' needs and coming up with the most suitable services for

1018 J. Hoover (note 988).
1019 See also Chapter 8.
1020 *Id.*
1021 J. Hoover (note 988); Norman Pelzl (note 65).

their needs, have often access to or an overview of customers' data. Therefore, they should also be considered as actors of the cloud business cycle and have their selves and their functions subjected to any rules put together for managing the internal aspect of cloud networks.

d. The innovative nature of cloud computing business and the legal challenges raised as a result thereof

The revolutionary elements cloud computing has by nature as a technology have also had their effect on the way business is done in the cloud market. We have already gone through novel roles and actors appearing in the business cycle of cloud computing and have also seen into what they do new or differently compared to the past[1022]. These innovations, in roles and tasks, have already ignited demand for original rules that will resolve issues unique to them. Apart from the points that have already been raised though, it is important to take a step back and look at the broader picture of the cloud market and business. Defined and clearly affected by the pioneering elements cloud computing inherently possesses, the way the relevant market sector works also offers interesting hints pointing to the way and characteristics that rules governing the cloud should have.

For starters, it is important to emphasize that the broader cloud computing business is characterized by several different types of varieties[1023] which are also characteristic of the cloud per se and are, therefore, becoming more and more prevalent in numerous areas of the IT economy that rely on cloud computing:

– Variety in norms: The cloud's standard order of business is defined by a plurality of state actors, greatly varying in size, magnitude and authority, ranging from national government agencies to supranational institutions[1024]. All these, equipped with a certain degree of formal rule making capacity have engaged in enacting a diverse set of (partly overlapping or otherwise interacting) norms aimed at regulating certain manifestations of the cloud computing phenomenon. Up to now though, their regulatory compass has left mostly untouched the essence of cloud computing per se, i.e. the cloud as a technology made possible

1022 See Chapter 2.
1023 Willcocks, Leslie P., Venters, Will and Whitley, Edgar A. (note 111).
1024 See Chapter 5.

thanks to a certain technological arrangement and as a workflow/ a lifecycle for any kind of digital or digitized data with several actors taking part or contributing to it and several exits from the cycle, each one marking one of those manifestations of the cloud towards its end users or recipients of the end-products of this workflow.

– Variety in control mechanisms: Due to the novelties it brought with, cloud computing has nurtured a great deal of new approaches to the issue of its regulation as a phenomenon. To a certain extent also because of the lack of concrete rules and laws governing the cloud per se, and further driven by the speed at which phenomena (i.e. applications, systems, products, services etc.) facilitated by cloud computing appear, there has been a plethora of alternative regulatory approaches to cloud computing[1025], besides traditional, hierarchical mechanism of control. Until now legal and regulatory approaches to cloud computing include alternative modes of control, such as market regulation, the shaping of social norms, and design requirements. All of these tools have resulted in the conception and establishment of a wide range of legal dicta regarding the cloud, which it is high time to be systematized and codified into a code of rules that will not necessarily replace of body of law we already have regarding manifestations of cloud computing but will work as the foundations for the entire construction of IT law.
– Variety in controllers: In the race to effectively regulate all manifestations of cloud computing and the applications it has given life to, traditional state regulatory bodies, namely government agencies or courts, continue to play a key role. However, the speedy and innovative evolution of the broader IT sector the cloud has made possible, also served as fertile ground so that important control functions be attributed to alternative governance institutions[1026], for instance standard setting bodies and trade associations. Of course, the regulatory competence of the latter is not on a par with that of full-capacity lawmakers. However, it should not fail our attention that many of them experience the cloud and the practices developed around and through it from much closer than conventional legislators. Without suggesting that they should fully and officially be made part of the law-making process with regard to rules on cloud computing (after all, law production as such is not yet

1025 See Chapters 3 and 4.
1026 See Chapter 6.

mature enough to undergo such a major makeover), it is definitely advisable to take what these actors have to say about how to effectively regulate the cloud seriously into account. As it has been demonstrated several times throughout this study, these alternative governance institutions are much closer to the inner, most fundamental aspects of the cloud computing phenomenon and already possess much more advanced ways of interpreting the cloud through interdisciplinary and, thus, more analytical lenses. To fully comprehend cloud computing, regulators need to profoundly grasp not just what computing results in for the real world but also what it actually is, how it actually works and on how many different dimensions (geographic, technical and jurisdictional ones) it is moving in parallel. Working hand in hand with such entities that can assist this quest for deeper Interdisciplinarity is key to successful and efficient cloud regulation.

– Variety in controllees[1027]: so far in the cloud computing related ecosystem of laws, businesses that provide cloud services to consumers have been the key regulatory subjects. However, as it has been extensively demonstrated[1028], a broader range of actors is relevant if we are to build up a holistic range of regulatory tools for the cloud. From those entities putting the cloud together, as infrastructure, to those setting the stage for cloud service providers to market their offerings to consumers, to actors facilitating access of the users to the APIs of cloud services, there is a long path with multiple players whose roles and functions have been so far insufficiently mapped and remain in a state of regulatory limbo. Even governments themselves play their part in governance efforts for the cloud, in the sense that, possibly for the first time in history to such an advanced degree, they need to outdo themselves and, without going as far as succumbing part of their sovereignty to some form of abstract supranational IT-dedicated legal order, they nevertheless need to develop cloud computing laws that will be able to plug into each other.

1027 Urs Gasser (note 959).
1028 See Chapter 8.

e. Summarizing the issues raised by the new modus operandi established in IT market by cloud computing; where is there a need for new cloud computing rules and what precisely should their content be?

The cloud market and the way it functions, as they have been extensively described and analyzed so far, have expectedly given rise to a heated debate about a series of key issues related to the cloud computing phenomenon. In previous parts of this study, we have already presented the main fronts on which the cloud computing reality has stirred debate and concern. Many of these issues are the product and result of the very architecture of the whole cloud market structure and of four basic risk factors on which it is founded[1029]: Outsourcing, centralization, internationalization and, as a result of the previous three, systemic complexity. Now that we have examined in such an analytical manner not only what issues the establishment of the cloud as standard IT technology has raised but also how it works and how the market created around it is functioning, it is worth summarizing those issues and arguing on which of them could be the subject matter of rules dedicated to regulating the cloud or which they are already dealt with by other pieces of legislation:

i. Data protection

Undoubtedly, data protection has been brought forward as the main issue to be closely watched and monitored as to the effects that can be brought upon it by cloud computing. There are several reasons behind this, namely the fact that since by definition cloud as a technology is almost always interrelated one way or another to data or that data protection has come, to a certain extent, to be regarded almost as synonym to 'risks posed by cloud computing' in public debate[1030]. We have already seen that, indeed, the architecture of cloud computing and the sensitive nature of data stored in cloud-based environments do raise concerns regarding individual rights and related safeguards, such as data quality, processing transparency, and international data transfers with good reason. It would be unfair to claim that legislators have failed to comprehend the urgency of the matter and work on legal tools that allow us to deal with this issue. However, just as

1029 Benoit Dupont (note 111).
1030 See Chapter 7.

the GDPR is on the countdown before coming into force in Europe and other such initiatives are also underway in the US, there has been rightful warnings voiced that, in our haste to safeguard our data as efficiently as possible, we are moving in the wrong direction. EU law is dealing with data as if these continue to be under the effective control of their owners[1031] in today's data technology landscape, while this is not entirely true nor is it the most efficient way to go after data protection. On the other hand, US law insists on the path of granting preferential treatment to government and state agencies regarding their possibility to get access to any of their subjects' data, while recent experience has proved that this is no longer safe (the technical lacunae that permit the state to get access to citizens' data could as well be exploited by others for malicious purposes) and it is growing less and less bearable by data owners[1032]. Our discourse so far and the exposure of what cloud computing is really about has only highlighted that, while it is absolutely essential to work on the front of data protection and maintain relevant rules updated at all times, it is high time to closely examine and regulate the actual medium and field where the whole game with data is played, i.e. the cloud networks themselves and cloud computing itself as the actual vessel for practically any computational process imaginable nowadays.

ii. Data Security

It is regarded by many that security issues are the second biggest risk the cloud has given rise to with regard to the countless amounts of data hosted on cloud network facilities[1033]. Consequently, issues such as data security standards, contractual rules, and legal obligations have risen among top preoccupations[1034]. Already, several specific problems have been brought to the forefront with equally numerous solutions that have been put to discussion. These include, for instance, digital signature legislation, breach notification laws, rules regulating how data can be stored in the cloud, se-

1031 See Chapters 6 and 7.
1032 See Chapter 3.
1033 Nicholas Platten (note 42).
1034 See also Chapters 5, 6 and 7.

curity audit requirements etc.[1035]. While on these topics there are already several legal options on the table, we are still missing the most crucial element, i.e. rules that will allow us to determine who is to bear the blame in case such security breaches occur and, most importantly, who is truly responsible at any given time to prevent such breaches from happening. The analysis of the inner architecture of cloud networks and the mapping of actors playing their roles across the cloud workflow only bring to surface the need for such dedicated cloud computing legislation, which will not cripple or render obsolete but it will rather help already existing IT laws become more focused and effective upon application.

iii. Data retention

One of the practices that thrived thanks to cloud computing but also because of modern challenges and policies such as economic regulation or national security obligations is retention of data with the use of cloud computing[1036]. Consequently, we are increasingly facing the challenge of balancing between the development, implementation, and operation of retention practices against civil liberties and other fundamental rights[1037]. For the time being, regulatory approaches trying to uphold these fundamental liberties against such practices are largely based on the theory of consent of the data subjects with regard to collection of data attributable to them. This is the default point adopted in the GDPR as well[1038] and it is, in generally, regarded as the next big frontier in the quest for empowering data subjects in their struggle to preserve their data. However, important as these steps may be, they fail to recognize one elementary fact about data in the era of cloud computing: from the moment when data enter the cloud, they are by default out of the data subject's control[1039]. Therefore, the burden of preserving the integrity of users' data, of determining when and under what conditions they could be handed over to third parties or

1035 Kenneth A. Bamberger & Deirdre K. Mulligan (note 968).; Urs Gasser (note 959).
1036 Eoghan Casey, Handbook of digital forensics and investigation (2010); Reilly, D., Wren, C., & Berry, T., Cloud computing: Forensic challenges for law enforcement. In Internet Technology and Secured Transactions (ICITST.)
1037 Paul Schwartz (note 155).
1038 See Chapter 4.
1039 Hassan Takabi, James B. D. Joshi & Gail-Joon Ahn (note 119).

state authorities or to what extent they should make it permissible for third parties to have access to users' data needs to transferred to the actors facilitating the cloud computing business workflow. Of course, it is certainly no harm for data subjects to maintain the prerogative of consent; however, without rules that will define who among the various actors handling users' data on the course of a cloud-based computational procedure is tasked with respecting users' choice in terms of that consent, the front of data retention will remain only partially regulated.

iv. Consumer protection

The rate at which cloud computing services are becoming the mainstream choice for virtually all groups of IT services consumers, from individuals to big-scale enterprise users, has subsequently given rise to a series of consumer protection issues in the cloud market[1040]. These concerns are mainly fueled in light of the fact that users of cloud services have to agree to prefabricated terms and conditions that apply to the services they wish to use. Additionally, it is common truth that communication between cloud providers and consumers or the feasibility of existing consumer protection laws to regulate these relationships are all characterized by information and power asymmetries[1041]. Improvements on that front are also to be expected; to a certain extent they are bound to happen as consumers will be pushing forward for their interests and will seek protection for them in more concentrated manners. However, the asymmetry between service providers and users of cloud services is most unlikely to cease to exist any time soon, if it can, at all. Therefore, it is again on the front of regulation of cloud computing per se where it is possible, via rules that will clarify which cloud actor is responsible for which specific tasks and duties at each time within the cloud business workflow, to partly outdo the difference of power observed between consumers and cloud computing service providers. Yet again, the proposed cloud-specific rules are not meant to substitute but, rather, to complement consumer laws with the aim of achieving the best possible balance between the two ends of the cloud market equilibrium.

1040 Kenneth A. Bamberger & Deirdre K. Mulligan (note 968).
1041 Paul M. Schwartz (note 157).

v. Intellectual Property

IP rights are of paramount importance on the cloud given that a great deal of all digital content available on the cloud is subject to intellectual property rules and can be of great financial value to right holders[1042]. From social media to the publication industry, the cloud hosts numerous activities, either digital since conception or converted into digital formats in order to adapt to modern demand, which involve materials subject to IP laws. The exploitation of intellectual property in the cloud environment is often fervently contested. For instance, low entry barriers for large-scale distribution of copyright protected content raises concerns about possible piracy on the side of rightholders. Strengthening IP rights and putting in place better enforcement mechanisms are among issues mentioned in most cloud policy debates[1043]. While it is true that modernizing and reinforcing IP laws can decisively contribute to better protection of relevant rights in the times of cloud economy, protection will not be complete before establishing rules that will define which of the cloud network actors are, at each time, charged with upholding those rights. In fact, cloud computing regulation should not stipulate just on cloud computing actors being deterred from offending the rights of their users (among which IP rights as well) but it should oblige them to actively take action towards better protection of them.

vi. Competition

Given the size and value of commerce and economic activity done on the cloud, it goes without saying that competition law and affairs would be stirred due to cloud technologies. In particular, the centralized nature of cloud computing infrastructures, questions of ownership, antitrust and, perhaps most importantly, interoperability issues have emerged[1044]. The thorniest problems are thought to be contractual concerns (e.g., adhesion forms of contracts), the lack of portability and conflicts between open and closed standards. Needless to say, competition issues raised as a result of

1042 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar (note 975).
1043 Paul M. Schwartz (note 157).
1044 Urs Gasser (note 959).

the introduction of cloud computing are too vast a field to be discussed on the sidelines of this study. However, it could be briefly argued that at the heart of the quest for a better functioning and with fairer competition conditions cloud market lies one predominant tool: interoperability. Given that the cloud economy is, to a great extent, founded on the flexibility with which users can go up or down on the amount of computational resources they use at any given time depending on their needs, it only makes sense that they should enjoy this flexibility not only within the resources of a specific service provider but also when transiting from one to the other. Cloud computing specific rules should definitely incorporate regulations regarding the minimum interoperability standards cloud providers should guarantee to their customers at all times and throughout the cloud business workflow. In addition, interoperability will be even further advanced if cloud computing laws are founded on similar principles on a cross-jurisdictional basis contributing to the advancement of fair competition, for the benefit of both service providers and customers, on a universal basis or, in any case, on such an extensive level as possible[1045].

vii. Trade

Although steps are constantly made towards bringing down such measures restricting free economic activity in the field of cloud computing worldwide, there are still several such procedures or requirements that hinder cloud business. For instance, there are several types of registrations cloud companies have to go through in a given country before they can provide services there (for instance, the EU-US Privacy Shield agreement that replaced the Safe Harbor agreement[1046]) that create trade barriers for cloud providers or the harmonization of government procurement rules. It would certainly be too optimistic or even unnecessarily bold to claim that merely

1045 Also refer to Chapter 11.

1046 The EU-US Privacy Shield is a framework agreement for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. One of its purposes is to permit US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union citizens. The EU-US Privacy Shield is a replacement for the International Safe Harbor Privacy Principles which were declared invalid by the European Court of Justice in October 2015 by virtue of judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner.

by introducing fundamental cloud computing laws such trade barriers could be totally abolished[1047]. However, in so far as the rules governing the functioning of the very cloud networks and their actors applicable in each jurisdiction are based on common core principles, obstacles to cloud computing business can be expected to be minimized.

viii. Jurisdiction, applicable law, enforcement[1048]

In order to make the most out of economies of scale, cloud computing heavily resorts to the flow of data across jurisdictional boundaries, be it at the local, national, or regional level[1049]. As it has already been analyzed, this potentially global flow of data naturally triggers questions of jurisdiction, applicable law, and enforcement. It has also been argued that, bold as that may be, it does not appear to be very realistic at this moment to move any time soon towards a regime of global regulation of cross-jurisdictional data flows[1050]. Even more, it is even questionable whether such a big leap from the existing jurisdictional status quo for the cloud to a substantially different, universalized one would make sense or whether it would be met with positive feelings from all affected parties, even if we suppose that it was achieved somehow. However, it is certain that jurisdictional frictions would be significantly softened if rules that dealt with the cloud market and the characteristics it and the entities active within it truly have are put in force. As these rules are proposed to be primarily founded on the teleological perspective[1051], they will definitely help to track down which actor of a cloud business workflow was responsible for what function at any given instance of the cloud workflow; once the entity upon which responsibility or culpability is attributable is identified, answering the question of jurisdiction and other neighboring topics will become an easier task.

1047 Margot Kaminski, *Why trade is not the place for the EU to negotiate privacy* Internet Policy Review (2015.)
1048 See also Chapters 6 and 7.
1049 See Chapter 6.
1050 See Chapters 5 and 6.
1051 See Chapter 5.

ix. Compliance[1052]

Cloud computing providers need not only to abide by general laws, but also to comply with an ever-growing body of very detailed sector-specific regulations (e.g., regarding financial, educational, or health data) and master the interplay among them, especially in instances of cross-jurisdictional nature. Similar to what has been argued before with relation to jurisdiction, rules regulating all that is happening on the internal aspect of cloud networks will help determine at each time which is responsible for what function during the computational process, thus making it easier to determine the entity responsible for upholding compliance requirements as well.

x. Transparency

This is the challenge with which a regulation specialized in the cloud could make a difference. Transparency and clarity are central concerns in the wider cloud environment touching upon a wide range of issues from contractual arrangements to regulatory approaches over a wide range of applications and manifestations related to the cloud as a technological, organizational, and economical phenomenon[1053]. The proposed rules, which are meant to primarily shed light and regulate what is actually happening in the day-to-day function of cloud networks and the business workflow that is made possible thanks to them, will decisively contribute to making the broad picture around cloud computing clearer and more transparent. By adopting rules that will help at each time to clear out who among a cloud network's actors is responsible for which of the events taking place within the cloud workflow, not according to a standard description of duties and tasks for each actor but as a result of an ad hoc analysis of processes that are underway, actors that are taking part in them and what role they are precisely carrying in any given time, chances augment that handling and regulation of affairs on any given instance will be conducted in a transparent and just manner.

1052 See Chapters 6 and 7.
1053 Nicholas Platten (note 42).

xi. Responsibility and liability[1054]

The proposed rules governing the internal aspect of cloud networks and the cloud business cycle will help, in a very similar manner to the one related to transparency, the need for fairer and more pragmatic allocation of responsibility and liability on the cloud. The great variety of instruments currently available in determining and allocating responsibility and liability over any harmful incident involving cloud technologies will be decisively better applied if reinforced by a set of rules on cloud computing with the nature and principles proposed hereby. Instruments for determining wrongdoing[1055] and liability in IT and, hence, in the cloud are numerous, ranging from traditional approaches (criminal law, civil liability, and risk insurance) to concepts such as corporate social responsibility. If coupled with a set of governance principles on the very functioning of cloud networks, their efficiency can do not worse than improve.

xii. Infrastructure

As it has been earlier discussed[1056] infrastructure of cloud networks, which is naturally the raw material for building the entire cloud phenomenon altogether, is needed in abundance as the use of the cloud spreads. Therefore, cloud computing providers heavily invest in more and more facilities of this kind across various geographical locations trying to optimize as much as they can, at the same time, any relevant economies of scale, i.e. by choosing locations for their server hubs which take advantage of favorable energy and climate conditions or which are within jurisdictions that offer attractive investment benefits for IT infrastructure providers to lay out their facilities within their limits. These jurisdictions do not necessarily belong to countries with generally well-developed and robust IT laws. Therefore, establishing rules which will permit us to track down responsibility all the way down to the infrastructure level can contribute, via the teleological and the principle of extra-territoriality, to legal safety overall in relation to using cloud technologies.

1054 Refer also to Chapter 7.
1055 Benoit Dupont (note 111).
1056 See Chapters 2 and 8.

f. What challenges lie ahead in designing cloud computing regulation rules?

In designing the proposed cloud computing regulations, lawmakers will have to make many choices in response to several questions regarding the cloud computing phenomenon and how several of its parameters should be regulated. As per every law-making procedure[1057], designing the bouquet of cloud computing rules is a process with three distinct phases, namely conceptualization, implementation and assessment[1058]. The challenges and optimal ways to tackle them are discussed hereunder in light of the analysis on the internal perspective of cloud computing.

i. Challenges in conceptualizing cloud computing regulation

Challenges during the conceptualization phase of cloud computing laws are basic "horizontal" challenges law makers are confronted with when considering the regulation of any technological innovation[1059]. In the case of cloud computing, three appear to be the main challenges based on the analysis so far: justification of law and regulation, trade-offs between policy objectives, and conflicts among the different roles held by governments in relation to the cloud phenomenon.

– Justification

In every law-making process governments or, in general, legislative authorities, have a certain range of mechanisms available to detect legal and regulatory issues related the subject matter of the laws they are about to design. As it is commonly admitted, what issues do finally make it onto the legal and regulatory agenda greatly depends on the prevailing political economy in which an issue, in this case cloud computing, emerges and diffuses; accordingly, these conditions may vary across countries. As far as the cloud is concerned, analysis[1060] so far has demonstrated that, although the two jurisdictions under examination in this study (i.e. EU and

---

1057 For an in-depth analysis of what risks building any system of laws inherently carries as a process refer to: Alden Heintz, *The Dangers of Regulation*, 29 J Communication 129–134 (1979.)

1058 Trevor Bench-Capon & Giovanni Sartor (note 956).

1059 John G. Palfrey & Urs Gasser (note 235).

1060 See Chapter 3.

the US) may be following distinctly separate routes in the way they handle IT and, in particular, data-related issues, in both of them there is a strong momentum in civil society for taking decisive measures and adopting laws that will clear out the current blurry picture when it comes to regulating cloud technologies. This unanimous call for action should be heard by regulators and, apart from being a call for them to act, it can also serve as a perfect tool in working on producing rules for the cloud that will be based on common principles and will, therefore, be possible to be presented to both jurisdictions with an increased likelihood of being met favorably and embraced by all affected actors.

Moreover, on the outset of every law-making process, identification of legal and regulatory issues through mechanisms such as horizon scanning typically includes an assessment of the need for intervention, for instance in case a market failure is looming or has already occurred. When it comes to the cloud though, justification of law and regulation especially targeted at it becomes more complicated due to the fact that there is plenty of anecdotal evidence but not much empirical data available yet on its precise impact in a given area of concern[1061]. However, as analysis has shown already[1062], while there are truly numerous regulatory tools touching upon different manifestations or applications of cloud technologies, there still remains a lot of insecurity and friction both among these various tools and among different jurisdictions. The reason for that is that we are still missing the connecting substance among all these rules, i.e. we have yet to put in place rules regulating the cloud itself. Once such rules come to exist, and especially if a certain degree of universality is achieved in relation to their founding principles, all pre-existing rules will blend better with each other.

– Trade-offs

The wider field of IT regulation has been an area where, in the process of designing laws, there is traditionally heated debate regarding tensions and, not rarely, trade-offs among values that are attempted to be promoted and

1061 Primavera De Filippi, Primavera De Filippi & Luca Belli, *Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation*, 3 European Journal of Law and Technology 156–173 (2012); Deepak Puthal, B.P.S. Sahoo, Sambit Mishra & Satyabrata Swain (note 837).; Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

1062 See Chapter 4.

underlying policy objectives[1063]. In the case of cloud computing, such friction is clearly visible whenever lawmakers seek to establish or strengthen frameworks aimed at enhancing consumer trust in cloud computing technology. For example, whenever an update process on privacy legislation is underway, in Europe or in the USA, it always goes hand in hand with the concerns that respective massive surveillance programs on behalf of states pose on that privacy. This had been particularly true, for instance, during the recently terminated negotiation process regarding the EU's GDPR, which faced a lot of turbulence in light of other legislative initiatives of the European Commission focusing on the issues of health research or banking to name a few[1064]. Actually, those parallel policies contradicting the values of privacy and confidentiality of electronic communications, among others, are usually targeting cloud computing services and providers of them 'incriminating' them in the eyes of users for the harmful events which they may have to eventually undergo. However, this often leads to a blurry picture as to who is responsible for preserving safety and security of data in the cloud, who is tasked with balancing between the objectives pursued by different laws which, however, aim to regulate the same subject matter (e.g. data transfers). The proposed regulatory scheme for cloud networks, which will put emphasis on clearing out which cloud actor is tasked with what specific duties at each time throughout the cloud workflow, will help to shed light also on the issues of responsibility for abiding with the plethora of laws regulating individual manifestations or uses of cloud computing. Moreover, the proposed set of principles for regulating the cloud should also touch upon the issue of superiority between conflicting rules affecting the same areas of cloud-related activity[1065] putting an end to the insecurities that still so manifestly exist despite an

1063 J. Hoover (note 988).

1064 For further analysis on the points of conflict between the GDPR and other regulatory initiatives of EU law refer to: Paul de Hert & Vagelis Papakonstantinou, *The new General Data Protection Regulation. Still a sound system for the protection of individuals?*, 32 Computer Law & Security Review 179–194 (2016); Dias, Renata Dalle Molle Araujo, *The Potential Impact of the EU General Data Protection Regulation on Pharmacogenomics Research*, 36 Med. & L. 43–58 (2017); John Mark Michael Rumbold & Barbara Pierscionek, *The Effect of the General Data Protection Regulation on Medical Research*, 19 Journal of medical Internet research e47 (2017); Alexander Roßnagel ed. (note 285).

1065 See also Chapter 11.

already wide range of legal tools attempting to deal with all outstanding issues in the wider field of IT.

– Role conflicts

The third most important challenge that will expectedly come up when designing laws regulating the cloud is, as it has become evident of the analysis in this and the previous chapter, the conflict of roles that the same actors are tasked with at different instances of the cloud computing workflow. In fact, role conflicts occur not only with regard to actors of the network but also on behalf of governments, in the sense of legislative, regulatory or executive bodies[1066]. An extensive review of broad cloud computing strategies implemented by governments around the world indicates that governmental bodies typically play more than one role in relation to the cloud[1067]. In fact, on most occasions, governmental organizations are simultaneously users, regulators, coordinators, promoters, researchers, even service providers within the context of cloud computing. This double pool of conflicts from the part of cloud actors and governmental authorities alike, calls for immediate settlement in the context of a regulatory framework for the cloud. As it has been argued earlier, putting in place rules that will answer the question of who is responsible for what within a cloud network not based on specific applications of the cloud, as case studies, but in a generic, role-description based manner, will decisively help in clearing out conflicting situations as these. To the extent that this is achieved, it will be beneficial not only for reinforcing the sentiment of trust to the law from users of cloud computing but it will also further encourage adoption of the cloud from stakeholders both domestically and internationally.

ii. Challenges in implementing cloud computing regulation

Beyond the conceptualization phase, drafting rules for the cloud is a process which is also possible to stumble upon a series of challenges most relevant to the implementation of these rules. Bearing in mind the analysis so far, three such challenges seem particularly noteworthy: problems with re-

1066 Stefanie Leimeister, Markus Böhm, Christoph Riedl & Helmut Krcmar (note 975).

1067 A. Froomkin (note 322).

gard to definitions, timing issues, and the challenge of appropriate tool selection.

– Metaphors and definitions

In any case of drafting rules for an innovative or unprecedented phenomenon, lawmakers and regulators typically resort to analogies or metaphors to understand and describe it[1068]. However, metaphors have the capacity to dictate regulatory thinking at the conceptual level and then influence approaches to the law at the implementation level. Similarly, the definitions used to describe this new phenomenon that is to be regulated or certain aspects of it can affect the way we approach these laws. So far, regulators wishing to define cloud computing in the context of any laws relevant to manifestations of it, confronted with the high degree of technicality and the fluidity in the cloud computing environment, have chosen not to develop their own technical definitions, but instead resort to definitions set forth by standard setting organizations. One such definition, which has been already discussed earlier in this study[1069], is the NIST cloud computing definition that was the proposed in the US Cloud Computing Act of 2012[1070], which sought to establish a new type of violation involving unauthorized access to computer systems in the Computer Fraud and Abuse Act[1071]. The proposal was met with criticism from legal scholars for its definitional vagueness[1072]. And this, despite the fact that the NIST definition of cloud computing is generally regarded as one of the most technically accurate regarding the cloud to date[1073]. Following the analysis presented so far, it is strongly recommended that a future regulatory framework for cloud computing should be based on a definition that will not only describe what cloud computing does, from a technical perspective, but also explain its dual nature as a concept, i.e. that it is not just about the external manifestations we see of it but also about the way the

1068 Trevor Bench-Capon & Giovanni Sartor (note 956).

1069 See Chapter 4.

1070 "S. 3569 — 112th Congress: Cloud Computing Act of 2012." www.GovTrack.us. 2012. November 8, 2016 https://www.govtrack.us/congress/bills/112/s3569.

1071 Refer also to Chapter 6.

1072 Goldman E., The Proposed "Cloud Computing Act of 2012," and How Internet Regulation Can Go Awry, available at http://www.forbes.com/sites/ericgoldman/2012/10/02/the-proposed-cloud-computing-act-of-2012-and-how-internet-regulation-can-go-awry/#7b0b6424113a; lastly accessed on 11/8/2016.

1073 See Chapter 4.

underlying technology and hardware are organized around certain actors to construct, all together, a dynamic and continuously changing business workflow. In this way, the subsequent rules will not only reflect on the external but also on the internal aspect of cloud computing dealing with the whole range of cloud-related issues calling for regulatory arrangement.

– Timing

Another critical question inherent with every law under development is the timing in which designated rules will intervene to settle the issues they refer to. In particular, when it comes to laws referring to rapidly changing areas of technology, determining the right timing when the negotiated provisions will apply is a critical factor for the effectiveness of them[1074]. As a result, lawmakers and regulators need to carefully consider timing issues when attempting to strike a balance between the creation of a friendly environment for cloud service providers on the one hand and safeguarding users on the other. Ideally, the relevant actors use a broad range of analytical tools in this process, including an assessment of the maturity of the technology, standards, and markets with strong network effects[1075], to name the most crucial ones. Throughout this study, it has been repeatedly argued that, while laws on the applications made possible thanks to cloud computing technologies usually adopt a punitive or repressive approach trying to describe in what way could harmful effects from malpractice with these applications could be limited, cloud computing regulation should adopt a primarily proactive approach focusing on who is charged with what functions and duties in that context throughout the cloud network. In this manner, it is expected that affected entities will be better aware of their duties and the preparations required to live up to depending on the role(s) they are playing within a cloud network, thus increasing the chances for smooth and transparent function of the cloud market and minimizing the odds for harmful events or spillovers thereof.

– Tool Selection

Last but not least, one key implementation challenge regulators invariably face when designing a law is to select the appropriate tool that is best suited to solve the regulatory issues or legal problems that had been pinpoint-

1074 Paul M. Schwartz (note 157).

1075 Gabriela Zanfir ed., What Happens in the Cloud Stays in the Cloud, or Why the Cloud's Architecture Should Be Transformed in 'Virtual Territorial Scope' (2013.)

ed and led to the formulation of a said piece of legislation[1076]. Truth be told, the fact that so far law making in the field of IT has been focusing on particular manifestations of IT technologies has resulted, for the moment, in lack of data which does not permit to immediately understand the contours of the problem of regulating the cloud itself in detail[1077]. Conversely, on the side of remedies, matching problems with tools repeatedly turns to be complicated by the fact that data about the performance of a given remedy in a specific context rarely exist in advance. In any case, given that we are talking about a sector with so many overlapping and interconnected phenomena, the use of a remedy tool with regard to each of them should align with the mix of policy instruments chosen by regulators for neighboring phenomena. Necessarily, putting in place and selecting the right tools requires considering a number of factors including political, technical or market contexts, to name a few. In response to this challenge, the proposed regulatory framework on the cloud should be constructed not with a view to replacing existing tools and remedies but with the aim of supplementing them, helping, particularly, to clear out the picture as to which remedy is more suitable and at whom among the different cloud actors it is addressable at any given time.

iii. Projecting challenges in the assessment phase of a regulation on the cloud

In the context of every law drafting process the latest step of work is to make a projection of the negotiated rules being applied and assess what will be the actual status quo in the field they aim to regulate after they enter into force. With relation to a potential law regulating the cloud the following are the main challenges regulators need to make an estimate about for the post-application period.

– Measures of success

The most common front where assessment challenges arise in law-making is that of establishing criteria with which it is possible to measure whether a law has been successful and at what extent[1078]. It is a fact that among different jurisdictions there is no generally accepted and stable set of crite-

1076 Urs Gasser (note 959).
1077 Benoit Dupont (note 111).
1078 Urs Gasser (note 959).

ria to evaluate the performance of various tools lawmakers and regulators have at their disposal across different regulatory contexts. In some cases, such criteria might focus on parameters such as coerciveness, directness, automaticity, and visibility[1079]. In others, criteria such as effectiveness, efficiency, and flexibility might rather be used[1080]. What is more, while at the moment a law is adopted everyone agrees that there should be constant evaluation of its effectiveness and, after a relative period of time since its introduction there should be an assessment as to the necessity of any modifications to it, more often than not these priorities atone or do not get much attention at all. Beyond instruments, it is often not clear what success means for a piece of legislation, in particular with respect to the outcomes of technology regulation. As it has been analyzed[1081], for instance, in one jurisdiction success for a law regulating data transfers can mean making it as conditional as possible to let any such transfer happen, while in another it can mean having corrective tools available for anyone that may suffer any kind of damage from one such transfer to amend it once it occurs. Moreover, the complexity of such normative questions regarding the result of regulatory interventions and whether it can be evaluated positively or negatively only increases where multiple tools regarding distinct but definitely adjacent manifestations of a wider phenomenon are at work simultaneously, or where a variety of instruments are used to pursue different and, at times, even conflicting policy objectives, as discussed before[1082]. It is possibly still too premature to know how regulating the very core of the cloud computing phenomenon will affect the overall functioning of the IT field. Nevertheless, bearing in mind the analysis so far and the fact that the proposed rules regarding the cloud from its internal perspective are not meant to replace but to supplement and fortify already existing legislation on the most important cloud-based phenomena and applications, two indexes could already serve as measurements regarding the success of cloud laws: on the one hand, the extent at which frictions over which jurisdiction takes prerogative over the others are alleviated. On the

1079 Coglianese, C., Measuring Regulatory Performance: EVALUATING THE IMPACT OF REGULATION AND REGULATORY POLICY, OECD, Expert Paper No. 1, August 2012, available at https://www.oecd.org/gov/regulatory-policy/1_coglianese%20web.pdf (lastly accessed: 11/8/2016.)

1080 Id.

1081 See Chapter 6.

1082 See Chapter 5.

other hand, given that the proposed principles on cloud regulation are meant to harmonize the effects of laws of different jurisdictions by respecting, at the same time, the different approaches each of these take on the same issues, a measurement of success for the proposed regulatory principles can be the degree at which the protective effect achieved within one jurisdiction is also deemed to be satisfactory under the standards of the other. If these two measurements do not reach adequate values, then even further refinement will be in order.

– Collateral effects

Regulation in general and all the more so regulation of such innovative phenomena as IT technologies can lead to collateral effects[1083]. A distinctive example of this type of challenge are the side-effects of the Digital Millennium Copyright Act in the US[1084], which was enacted aiming – among others – to put in place additional layers of protection of copyrighted works, but has been arguably used in ways totally unintended by the legislator. In the case of rules regulating the cloud from the internal perspective, the most likely collateral effect is the one most common with reference to any piece of IT legislation, i.e. the possibility that it may fail to comprehend the way technology will evolve and become soon ineffective or create legal voids that could be exploitable in unintended manners[1085]. However, this is a possibility that can never be totally taken off the table; the soundest advice IT regulators should always bear in mind is that rules referring to such dynamic phenomena as IT technologies require from them constant high alert and a keen eye to spot whenever the time has come for the next update. Besides, the fact that the proposed rules are not meant to extend to external manifestations of the cloud but touch only its internal aspects guarantees that, so long as cloud computing remains the standard facilitating IT technology, the rules on it can only work to the benefit of both technological progress and users' interests at the same

---

1083 Trevor Bench-Capon & Giovanni Sartor (note 956).

1084 The Digital Millennium Copyright Act (DMCA) is a US copyright law implementing two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works. It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, it heightens the penalties for copyright infringement on the Internet. Pub. L. 105-304; 112 Stat. 2860 (1998.)

1085 Chris Reed (note 363).

time. The aim is to regulate the cloud not in order to disrupt it but in order to better streamline its capacities and channel them in ways that will maximize their positive while decreasing their negative potential.

– Ability to learn

Regulating such a state-of-the-art phenomenon like cloud computing, always calls for an assumption of uncertainty. The cloud computing legal and regulatory environment is characterized by high degrees of technical complexity and fast changing market conditions, to name only a few of its volatile aspects[1086]. These combined with the rest of the conceptual, implementation, and assessment phase challenges bring to the surface the need for regulatory systems to incorporate feedback channels, and mechanisms of self-assessment and correction[1087]. Putting in place such safeguards is anything but trivial for the longevity of cloud computing regulation. Options so far have included sunset clauses, periodic reviews, and consultation mechanisms[1088], but often these prove to be either relatively crude or not adequately flexible to live up to the speed of evolution of high-end technologies and corresponding market dynamics; the long-lasting review process of technology-relevant European Union legislation, only recently verified through the labyrinthine process of adoption of the GDPR is indicative thereof. Adopting rules on the cloud with the features and generic nature proposed in this study will not solve this challenge per se but will definitely set in motion a very crucial process towards the corroboration of IT law as an independent legal discipline. Rules focusing on the internal aspect of cloud networks could serve as the missing link that will ignite the chain of events that will offer to IT laws as a body of legislation the systematization and coherence they are currently missing, as it will be argued in the conclusions of this study.

1086 See also Chapters 2 and 8.
1087 J. Hoover (note 988).
1088 Coglianese op cit n 128 supra.