KIND Knowledge Innovation Network Dynamics Research Group
Institut Mines-Télécom, Télécom Ecole de Management

TELECOM Ecole de Management
Managing through Technology

Paper to be presented at the International Conference on

Organizations, institutions and innovation in the ICT sector: Where do we stand?

Conference organized by Institut-Mines Télécom,
Télécom École de Management
in Paris, 25-26 June 2012

Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation

Primavera De Filippi
CERSA / CNRS / Universit Paris II

Luca Belli
CERSA / CNRS / Universit Paris II

Law of the Cloud v Law of the Land:

Challenges and Opportunities for Innovation

I. Cloud Computing and Fundamental Rights

Although an exact definition of Cloud Computing has yet to be established,[1] it can generally be regarded as a set of technologies that enable the dynamic provision of computing resources over the Internet.[2] These can be either hardware resources - such as storage capacity and processing power[3] - or software resources - such as platforms and applications.[4] These resources are provided dynamically on-demand, automatically growing or shrinking according to actual needs - thereby reducing the risk of shortage or excess capacity. With the advent of Cloud Computing, an increasing number of applications are nowadays run in the Cloud rather than on user's devices. Most of these applications can be accessed through a simple web browser: this is the case of most web-mails, web-based document storage, as well as many web-based production and collaboration tools.

The main advantage of Cloud Computing for end-users is that data becomes accessible from anywhere and at any time, as long as there is an Internet

---

1 For a preliminary attempt to provide a systemic overview of Cloud Computing technologies, see e.g. Youseff, L. Toward a Unified Ontology of Cloud Computing, Grid Computing Environments Workshop, 2008. GCE '08

2 For a more accurate description, see the NIST definition of Cloud Computing, as ""a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [NIST Special Publication 800-145]

3 Cloud computing technologies provide users with the ability to acquire the technical infrastructure - in terms of storage, memory and processing power - dynamically and on demand. This is the most basic form of Cloud Computing, often referred to as IaaS (Infrastructure as a Service).

4 PaaS (Platform as a Service) and SaaS (Software as a Service) are more complex forms of Cloud Computing, which provide users with a computing platform - in the case of PaaS - typically including an operating system, a programming environment, a web server and a variety of databases - or, in the case of SaaS, an interface to computer software or other online application that do no longer need to be run on the end-users devices.

connection. This is likely to promote collaboration amongst users and facilitate data sharing across multiple locations. Cloud Computing also greatly reduces the costs of storing and processing information. Thanks to Cloud Computing technologies, a smart phone connected to the Cloud can be as powerful as a personal computer. Indeed, being most hardware and software resources increasingly relocated into the Cloud, users no longer need to purchase sophisticated computers with a large amount of resources; they can merely subscribe to a Cloud service, thus only paying for the amount of resources they use.

However, to the extent that they lose control over the technological infrastructure, software applications, and data stored in the Cloud, users can no longer govern the manner in which these resources can be accessed or used by them or by others. Conversely, by controlling the underlying architecture of the Cloud, Cloud providers acquire the ability to monitor the activities and communications of users, as well as to control, restrain or manipulate anything that enters into the Cloud.

Such a centralised infrastructure might negatively affect the fundamental rights of users, endangering their privacy and potentially jeopardizing their freedom of expression. In fact, to the extent that it has been stored in the Cloud, data could theoretically be disclosed (either deliberately or accidentally) to unauthorised parties. Cloud Computing can therefore have serious implications on the privacy of personal information and the confidentiality of corporate or governmental information.[5] Users' privacy is affected insofar as users will disclose information - either explicitly or implicitly through their actions - which can be characterised as sensitive personal data. Such data can subsequently be analysed, processed, and potentially exploited by Cloud providers, for purposes that often go beyond what is necessary to provide a service to their user-base.[6] The confidentiality of information stored in the Cloud is also put at risk to the extent that it subsists on remote servers held by a variety of market operators, who might have economic interests and/or legal obligations to disclose confidential information to third parties - be them commercial actors or governmental bodies.[7]

As a general rule, given the number of actors involved in the provision of a Cloud service, the risks of losing data or losing control over online information are much

---

[5] Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Report prepared by Robert Gellman for the World Privacy Forum, February 23, 2009

[6] For a survey of the various dangers and challenges for privacy in Cloud Computing environment, see Rong Zhang ; Wei Xie ; Weining Qian ; Aoying Zhou, Security and Privacy in Cloud Computing: A Survey, Sixth International Conference on Semantics Knowledge and Grid (SKG), 2010.

[7] Stephen S. Yau, Ho G. An, Confidentiality Protection in Cloud Computing Systems, in International Journal of Software and Informatics, Vol.4, No.4, December 2010, pp. 351–365

higher - and the impact much greater - in the context of Cloud Computing.[8] To ensure that users privacy and confidentiality are preserved, Cloud operators need to incur the infrastructural costs and adhere to specific duties of care in order to guarantee the security and integrity of online communications.[9] In addition, given the transnational character of Cloud Computing, a number of challenges must be addressed to determine the applicable law and the extent to which users' rights will be effectively protected. In certain jurisdictions, for instance, information stored in the Cloud may be accessible by governmental agencies, in spite of the rights and protections guaranteed under domestic law.[10]

Freedom of expression might also be significantly challenged by the advent of Cloud Computing. Since all communications passing through the Cloud can be easily monitored,[11] they can potentially be censored by the infrastructure provider. When Facebook declared that it was forbidden to post pictures illustrating naked breasts, many mothers had their breast-feeding pictures removed from their Facebook profiles without any opportunity of challenging this decision.[12] It could be argued that every online service provider has the right to decide what kind of content can be published on its own platform. Yet, given that, as a result of network effects, there are only a few platforms available for users to choose from, the arbitrary decision of any service provider holding a dominant position in the market might have negative effects on user's freedom of expression insofar as it only authorises certain types of communication.

Given the extent to which they can affect users' ability to communicate, the internal policy of Cloud service providers and the technical implementation of the

---

[8] S. Ovadia, Navigating the Challenges of the Cloud, in Behavioral & Social Sciences Librarian Volume 29, Issue 3, 2010

[9] Pearson, S. Taking account of privacy when designing cloud computing services, ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009. CLOUD '09.

[10] As an instance, the U.S. Patriot Act affects every services provided by U.S. companies, regardless of where the data centres are located, see Zack Whittaker, "Case study: How the USA PATRIOT Act can be used to access EU data"

[11] By exporting their data and their computing resources into the Cloud, users progressively lose control over their hardware and software resources, but also over the privacy of their communications. Indeed, Cloud providers can monitor and analyse all activities and communications performed by their users insofar as they necessarily have to connect into the Cloud in order to benefit from the service. For a more detailed overview of the issues related to data logging and monitoring in Cloud Computing, see e.g. bH. Takabi, Security and Privacy Challenges in Cloud Computing Environments, Security and Privacy, IEEE, Volume 8, Issue 6, Nov-Dec 2010

[12] Facebook claimed that pictures illustrating a "mother breastfeeding without clothes" were in violation with its terms of service according to which it is forbidden to post any "pornographic" content, or any image containing "nudity". For more details, see Facebook's Statement of Rights and Responsibilities available at http://www.facebook.com/legal/terms

user interface can produce normative governing effects similar to laws. However, as opposed to the *Law of the Land*[13], which must necessarily be enforced by appropriate authorities, the *Law of the Cloud* can be automatically enforced by the technical functionalities provided by the platform – which can be used either to enhance or to impede basic freedoms. If it is true that, as stated by Lawrence Lessig, "Code is law"[14], it is also true that the private policy of Cloud operators could be seen as a substitute legal system. These policies do indeed integrate a series of rules, which can be automatically imposed upon users by private enforcement systems and technological measures of self-help.[15] If the "medium is the message",[16] whoever controls the medium also has the possibility to control the contents of the message – either by modifying the technical infrastructure in order to indirectly affect the manner in which people communicate, or by interfering directly with users communication so as to censor, or eventually alter the content thereof.

Finally, anonymity is also likely to have a strong impact on freedom of communication. Since the right of freedom of expression also comprises the right to communicate anonymously, every user who communicates by means of an online application should be guaranteed that the service provider does indeed respect and enforce the anonymity of communications - a precondition for free political and social discourse.[17] Yet, for a variety of reasons - technical or not - Cloud providers tend to require users to identify themselves before they can benefit from their service. This is likely to trigger a chilling effect on communication and to limit users' ability to fully exercise their right to freedom of expression on the Internet.[18]

---

[13] The expression "Law of the Land" refers to the complex of laws in force in a given country. Such an expression finds its roots in the 1297 Magna Carta and has been reiterated in several Constitutions. For instance, the Supremacy clause in the United States Constitution states: "*This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the authority of the United States, shall be the supreme Law of the land*[...]"

[14] Lessig L., Code: And the Other Laws of Cyberspace, Version 2.0, 2006.

[15] See, e.g. Radin, Margaret Jane, Regulation by Contract, Regulation by Machine. Journal of Institutional and Theoretical Economics, Vol. 160, pp. 1-15, 2004.

[16] Marshall McLuhan coined the sentence "The medium is the message" to express the idea that the distinctive characteristics of a medium are necessarily embedded into the message it conveys to the extent that it influences how the message is perceived.

[17] Indeed, according to the United States Supreme Court, "[p]rotections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views [...] Anonymity is a shield from the tyranny of the majority". See: McIntyre v. Ohio Elections Comm'n (93-986), 514 U.S. 334 (1995).

[18] See the EFF report on Freedom of Expression, Privacy and Anonymity on the Internet, submitted to the United Nations Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression, January 2011

II. Cloud Computing and the Market

According to market economics, it might be assumed that the aforementioned problems could - theoretically - be ignored, since market mechanisms will make sure that no service provider will ever infringe the rights and the privacy of users beyond what is acceptable by them. In a competitive market, a service provider that does not respect the expectations of its user-base will eventually be overtaken by the operators that meet the demand of unsatisfied users. Competition will thus ensure that the fundamental rights of users are respected to the extent necessary as to satisfy the demand.

In practice, however, the advent of Cloud computing is characterised by a trend towards a massive centralization of resources.[19] In order to achieve significant economies of scale, large data centers have been developed, gathering together a large number of computing resources - in terms of storage capacity and processing power. While this is not a problem as such, centralisation could lead to market failure to the extent that the Cloud industry becomes dominated by a single entity or by a group of entities acting collectively. Should these entities abuse their dominant position, the self-regulating mechanisms of the market would most likely be compromised.[20]

By raising up market barriers, dominant players can limit the number of competitors in the market so as to maintain a dominant market share. This can be done, for instance, by reducing interoperability in order to lock users into a specific system and/or by acquiring priority access to the network so as to reduce the perceived quality of competing services. Given their consequences on innovation, those two mechanisms will be explored more in detail in the following sections.

---

[19] Qi Zhang Lu, Cheng and Raouf Boutaba, Cloud Computing: state-of-the-art and research challenges, in Journal of Internet Services and Applications, Volume 1, Number 1, 2010.

[20] In European competition law, the conduct of the dominant entity is considered as abusive when it results in competitors' exclusion that is likely to harm consumers' welfare. According to article 102 TFEU, "[…] Such an abuse may consist in: (a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;(b) limiting production, markets or technical development to the prejudice of consumers;(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage; (d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts"

A. Interoperability v User lock-in

Interoperability is generally regarded as a key factor for competition. In the European Union, interoperability emerged as a competition issue in the ICT sector as far back as the 1980s, with the *IBM* case,[21] and was reiterated in 2004 by the Court of First Instance which confirmed an infringement decision against Microsoft for failing to supply interoperability information to its competitor.[22] In addition, by virtue of the *Intel/McAfee* case, interoperability – notably, "degradation of interoperability" – gained a prevalent role in EU decisional practice.[23] On June 2010, the Vice President of the European Commission Joaquín Almunia underlined that the ICT sector is characterized by potentially strong network effects and strong risks of user lock-in which justify a growing need for interoperability.[24]

Nowadays, interoperability and data portability play a pivotal role in avoiding vertical integration and consumer lock-in - two frequently uttered risks with regard to Cloud Computing, where interoperability limitations have already been ascertained as potential causes of anti-competitive behaviors.[25] Thus, in order to ensure that consumers can freely chose and switch across the most competitive services, data portability and interoperability must necessarily be guaranteed.

Yet, Cloud providers are frequently tempted to lock their users into their system by increasing the transaction costs necessary to shift from one service to the other. This is generally done by relying on a proprietary system that does not allow for any kind of interoperability with competing services, or by means of contractual provisions imposed upon the user-base. By doing so, Cloud providers

---

[21] In the IBM case, Article 86 (now Art. 102 TFUE) infringement proceedings were brought against IBM by the EC. At the time, IBM was said to hold a dominant position in the supply of central processing units (CPUs) and operating systems, the two components of its System/370. See: Commission Decision 84.233.EEC, Official Journal of the European Communities L 118/24.

[22] See: Case T-201/04, Microsoft v Commission, Judgment of the Court of First Instance (Grand Chamber), 17 September 2007.

[23] The interoperability undertakings provided by the parties consist of: (i guaranteeing the access of interoperability information to vendors of rival security solutions; (ii) committing not to actively impede other security solutions from running on Intel's CPUs and (iii) committing not to hamper the performance of McAfee's security solutions on CPUs manufactured by Intel's competitions. See: Case COMP/M.5984 - INTEL / MCAFEE, Official Journal of the European Communities L 24, 29.1.2004

[24] See : EUROPA - Press Releases – "New Transatlantic Trends in Competition Policy Friends of Europe," 10 June 2010

[25] See: Case T-201/04 Microsoft Corp. v. Commission of the European Communities, ECR II-4463

can reduce the value (or the perceived value) of competing products without actually increasing the value of their own - a practice which can be considered abusive insofar as they hold a dominant position in the market.[26]
Such behavior has recently been ascribed to Google by virtue of its AdWords search advertising platform and AdWords Application Programming Interface (API).[27] In fact, by imposing contractual restrictions prohibiting the development of software to export data from AdWords to any alternative advertising platform, AdWords's Terms and Conditions introduced a considerable barrier to the utilisation of any competitive platform.[28] This affair illustrates how interoperability limitations can be used to trigger unnatural network externalities,[29] leading to an irregular augmentation of Google's market share to the detriment of its competitors, so as subsequently increase its market value.

To avoid similar problems, the proposal for the new Data Protection Regulation in Europe introduced provisions for data portability imposing that users are given the opportunity to retrieve their data in a "structured and commonly used" electronic format.[30] Yet, by neglecting to impose an obligation to provide data in an open format allowing users to transfer data to any other system of their choice, the Regulation does not however constitute a strong affirmation of the right to data portability.

---

[26] Abuse of dominant position may occur when a company behaves, to an appreciable extent, independently from its competitors, customers and consumers, while setting prices and other competitive parameters. See: paragraph 10 of the Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, Communication from the Commission [2009] Official Journal of the European Union, C 45/7

[27] On November 30th 2010, the European Commission launched an antitrust investigation into allegations that Google Inc. has abused a dominant position in online search, in violation of European Union rules (Article 102 TFEU). See: Europa Press release IP/10/1624, Brussels, 30 November 2010.

[28] Indeed, AdWords provisions exclusively allow manual data-transferring and data-comparing which are incredibly time-consuming and may trigger a considerable amount of errors, subsequently discouraging advertisers from using alternative platforms.

[29] Network externalities, also called network effects confer a considerable competitive advantage to the firm that owns the network. "This incumbent advantage arises because a new entrant must persuade people to join a network that starts with fewer members, and thus may be less valuable to them than the network they are currently in. This is why markets for products with network effects are often dominated by only a few firms or a single monopoly". See: Bishop M., "Essential Economics", Bloomberg Press, Economist Books, 2009.

[30] Article 18 introduces the data subject's right to data portability, i.e. to transfer data from one electronic processing system to and into another, without being prevented from doing so by the controller. As a precondition and in order to further improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format.

B. Net neutrality v bandwidth balkanization

On the Internet, a natural barrier to entry exists in the form of network effects - where the value of a service ultimately depends on the number of people using it. Every new user of the service creates positive externalities to the extent that it increases the value of the service as perceived by others. The greater is the number of users, the more valuable becomes the service. Eventually, a positive feedback loop can be observed, whereby the number of users renders the service more valuable and consequently attracts more users to join. Yet, such a virtuous cycle can only be achieved after a critical mass of users has been reached.

In the context of Cloud Comupting, network effects are especially relevant in the case of online social networks such as Twitter, Facebook, or Google+ whose utility increases as more users use it. The challenge for those online service providers is to attract as many users as possible in order to acquire the initial number of users necessary to trigger the *bandwagon effect*.[31]

Yet, the greater is the number of users, the more considerable will be the amount of data to be transferred within a given period of time. Given a limited amount of bandwidth, as the data flow increases, connection speed will necessary decrease. Nowadays, as the number of Internet users keep growing, bandwidth has become to be regarded as an increasingly scarce resource.
Cloud providers thus have an obvious incentive to pay more to get higher quality Internet connection. This can be achieved, in particular, through the technique of data prioritization[32] - by providing priority access to the network to only certain online intermediaries, thereby making their service more attractive to users and further increasing network effects. However, as will be highlighted below, being bandwidth a scarce resource, data flow prioritization may ultimately lead to the detriment of non-prioritized players.

---

[31] The bandwagon effect - also known as the copycat behavior - describes a situation whereby users' preference for a service increases with the number of users using it: the probability of any user adopting a service increases with the proportion of users who have already adopted it. Users' demand is no longer based exclusively on individual preferences or product quality, but is ultimately driven by other users' behavior. This situation may impair competition in the market, potentially leading to a situation of monopoly where "the winner takes it all."

[32] Recent developments in data flow management have led to the deployment of new tools allowing data prioritization through various techniques - e.g. Deep Packet Inspection (DPI), Data Shaping, etc. See: Picot A. Cave M., Workshop Next ("Now") Generation Access (NGA): How to Adapt the Electronic Communications Framework to Foster Investment and Promote Competition for the Benefit of Consumers?, 2008.

Since the transmission of data is a prerequisite for the provision and/or the consumption of Cloud services, Cloud providers and Internet users require a constant and reliable Internet connection provided by Internet service providers. ISPs thus find themselves in a highly strategic position along the Internet value chain, as they fundamentally constitute a two-sided platform, giving the opportunity to two different user groups - Internet users and Cloud providers - to benefit from each other.[33]
Data flow management tools might enable ISPs to implement data discrimination by means of Deep Packet Inspection (DPI) and other techniques commonly implemented in Next Generation Networks (NGN).[34] While it has been strongly criticized by net neutrality advocates,[35] data discrimination might actually bring a series of benefits to users eager to enjoy higher quality services on the Internet. Indeed, users generally consider it advantageous to get faster access to certain Cloud services so as to be able to upload and download data more quickly.

In light of these new traffic management possibilities and considering that users' demand for priority access to particular online services often implies data discrimination, this technique might eventually be integrated in the business model of a number of ISPs. This possibility has been officially acknowledged by the Vice-President of the European Commission Neelie Kroes who has clarified that the European Commission do not want to "c*reate obstacles to entrepreneurs who want to provide tailored connected services or service bundles*" though stressing that consumers must be "*aware of what they are getting, and what they are missing*"[36].

In the context of Cloud Computing, in order to cope with the considerable augmentation of bandwidth consumption determined by online services –

---

[33] See: Rochet J.-C. and Tirole J., « Platform Competition in Two-Sided Markets » in Journal of the European Economic Association, 2003.

[34] According to Picot, "Next Generation Network (NGN) is a concept describing a new architecture for electronic communications with unprecedented capacity and flexibility. NGN is throughout based on the Internet Protocol (IP). Thus, NGN is able to offer multiple services (e.g. voice, data, multimedia; synchronous, asynchronous; mobile, fixed; broadcast, point cast) over a single platform independent of underlying physical technology (fibre, coax, copper, radio). Compared to traditional (and presently still prevailing) Public Switched Telephone Networks (PSTN) and other dedicated specialized networks NGN is by far more efficient because it integrates all former networks and because it can deliver its powerful services based on a much less complex architecture (number of nodes, service and management needs)". See: Picot A. Cave M., op. cit.

[35] See, for instance: La Quadrature du Net, "Protecting Net Neutrality in Europe", 2009

[36] See: Kroes N. Next steps on Net Neutrality – making sure you get champagne service if that's what you're paying for May 29th, 2012.

particularly with regard to audiovisual applications[37] – ISPs can theoretically adopt three different approaches: (1) imposing constraints on the amount of data that can be transferred throughout the network, thereby decreasing the quality of the provided services, (2) undertaking network-improvement investments at the expense of end-users, e.g. by raising Internet fees (3) introducing better Internet traffic management, e.g. by introducing data discrimination.
The latter seems to be the most seducing option for ISPs. Indeed, by introducing data packet prioritization policies, ISPs could benefit from a more efficient management of their network, while offering both users and Cloud providers a wider range of options based on a variety of quality-of-service (QoS) parameters.

While enabling Cloud providers to provide faster and more reliable services to their customers, data discrimination may, however, also trigger anti-competitive behaviors and encourage the implementation of abusive business models. Offering priority access to the network to certain players only would most likely introduce a new barrier to entry - making it difficult or impossible for others to compete on equal grounds.[38] Access prioritization may thus jeopardize competition in the market, by precluding other service providers from offering a competing service without acquiring priority access for themselves. Regardless of the quality of the service they might offer, their services will, in fact, always be slower and therefore less valuable. Hence, if priority agreements between Cloud providers and ISPs were to be permitted, competition on the market for online services may be considerably compromised, to the ultimate detriment of end-users.

This is probably by reason of a similar reflexion that the European Parliament and the Council found it necessary to address the issue of network neutrality[39] while elaborating the Telecoms Package.[40] Although the principle of net neutrality has not been fully endorsed by European legislation, it has nonetheless been recognized as a useful means to promote competition and transparency in the

---

[37] See: "Cisco Visual Networking Index, Forecast and Methodology: 2009-2014", 2010; with regard to mobile Internet, see: "Cisco Visual Networking Index, Global Mobile Traffic Forecast", 2011

[38] Of course, the impact of packet discrimination may depend very much on the type of data that is being transferred. For instance, in the case of word processed files, a slight delay (e.g. milliseconds) in accessing it from the Cloud would probably not pose a problem to the user, however, in the case of video streaming or voice over IP, an excessive delay in the data flow would become undesirable.

[39] On October 6th 2009, the former European Commissioner for the Information Society, Viviane Reding affirmed that "the European Commission attaches high importance to preserving the open and neutral character of the net in Europe, in the interest of fair competition and tangible consumer benefit". See: " The Future of the Internet and Europe's Digital Agenda Lunch debate on the future of the Internet and Europe's digital strategy", Brussels, 6.10.2009

[40] The expression "Telecoms Package" refers to both Directive 2009/140/EC of the European Parliament and Council and Directive 2009/136/EC of the European Parliament and Council.

market for online services. It can be said, therefore, that the principle of network neutrality has been implemented *a minima* within European law. Without precluding the possibility for ISPs to implement innovative business models based on data discrimination, the European legislators endowed national regulators with the authority to decide the extent to which net neutrality should be protected. National Regulatory Agencies (NRA) have thus been empowered with the faculty to establish a minimum quality of service threshold[41] and to impose transparency obligations for network operators[42] in order to protect users' rights by making them aware of (and sometimes forbidding) certain kinds of network management practices.

Though not expressly endorsing the principle of network neutrality, the current approach presents the undeniable advantage of encouraging the experimentation of innovative business models, while ensuring that fair competition is preserved to the extent that users are properly informed of the limitations that they might encounter while using the service. Minimum quality thresholds can also be introduced to guarantee a preliminary implementation of the network neutrality principle, without overly constraining the contractual freedom of market players.
On the downside, it should be stressed that the Telecoms Package has however failed to achieve harmonization across Member States by neglecting to impose a coordinated approach establishing a common minimum quality threshold at the European level - opting instead for a more fragmented approach which presents the risk of "quality balkanisation" due to the potentially divergent minimum standards defined by different NRAs. To this latter extent, the Body of European Regulators for Electronic Communications (BEREC) might play a pivotal role in coordinating the different NRAs with the aim to harmonize the minimal standard of Internet connectivity.

The net neutrality approach chosen by the European Legislator has shed light on the necessity of envisaging a heterogeneous regulatory strategy in order to frame and best regulate the Cloud Computing phenomenon. The following section will analyze the different regulatory techniques that have been proposed so far, investigating their corresponding advantages and drawbacks to eventually come up with the most suitable solution.

---

41 See : Article 22(3) of the Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJ L 108, 24.4.2002

42 According to article 21.3.b of Directive 2009/136/EC, "Member States shall ensure that national regulatory authorities are able to oblige undertakings providing public electronic communications networks and/or publicly available electronic communications services to inter alia: [...] inform subscribers of any change to conditions limiting access to and/or use of services and applications, where such conditions are permitted under national law in accordance with Community law".

III. Regulatory solutions

Cloud computing is one of the most versatile and rapidly evolving segments of the Internet, allowing a plethora of different usages and combining a number of innovative technologies. Despite the relevance of Cloud Computing in the European economy,[43] no specific pan-European regulation has been elaborated so far. It is nonetheless possible to identify three different legal regimes affecting the Cloud Computing sector:[44] electronic communications regulation (cf. the Telecoms Package), electronic commerce regulation (cf. the Electronic Commerce Directive)[45] and European competition law.

As previously illustrated, the specificity of Cloud Computing is that it is a sector characterized by large economies of scale and strong network effects - which constitute an incentive towards the centralization of resources. The market for Cloud Computing services will thus inevitably be dominated by a few very large players, which may or may not be tempted to abuse their dominant position in the market.
Assuming that, once a dominant player is established in the market, the latter is no longer able to regulate itself efficiently, governmental intervention might be required in order to rectify market failures, ensuring that users are free to chose the service that best satisfies their needs. The fundamental question is, then, whether competition should be preserved through ex-ante or ex-post regulation. The former approach would suggest strengthening fundamental rights protection and/or introducing a strong net neutrality rules in the form of non-discrimination obligations, whereas the latter option would suggest using the judiciary tools that are already available under competition law and other bodies of law, such as privacy and consumer protection laws.

It should be stressed that, with regard to fundamental rights, were current data protection rules and consumer protection laws to be respected, users' rights would be properly upheld. However, the brief though intense history of the online industry has shown that fundamental rights protection - especially concerning privacy - has not been overwhelmingly successful. The strong criticism that the

---

[43] See: Europa Press release, "Digital Agenda: Commission outlines action plan to boost Europe's prosperity and well-being", IP/10/581, Brussels, 19 May 2010

[44] See: Sluijs J.P., Larouche P., Sauter W., Cloud Computing in the EU Policy Sphere, TILEC Discussion Paper, 2011.

[45] See: Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2000] Official Journal of the European Union, L 178/1

current European data protection regime has been subject to[46] has led to the development of a new data protection framework provided by the recently proposed Data Protection Regulation (DPR).[47] Aimed at strengthening users' fundamental rights, the adequacy of the new DPR remains however questionable. This is especially true in the context of Cloud Computing - characterized by a large number of actors, whose international scope makes it difficult to determine the applicable laws in the case of litigation. While its provisions apply to any entity processing EU citizens' data (regardless of their physical location),[48] the DPR does not however provide explicit protection against unauthorized access to EU data stored in a foreign data center by governmental authorities. EU citizens exporting data into the Cloud cannot in fact rely on data protection rules provided for under domestic law vis-à-vis foreign public authorities.[49]

Comment [1]:

Interoperability and data portability are two other factors that could enhance competition in the European market for Cloud services. In fact, the greater is the level of interoperability, the greater will be the portability of data amongst different Clouds services. In order to reduce the risks of consumers being locked into one particular online service, interoperability might however need to be enforced more sharply that it currently is under the revised Data Protection Regulation.[50] Indeed, by introducing interoperability obligations for Cloud operators - in addition to current data portability requirements - the law would enable users to export their data from one Cloud to another without any difficulty.

---

[46] See, for instance: Yankowitz J. More Crap From the E.U. in Information, Law, and the Law of Information, available on http://blogs.law.harvard.edu/infolaw/; The Wall Street Journal, Assessing the New EU Data Bill's Unforeseen Consequences, January 26, 2012.

[47] See: Europa Press release, "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, IP/12/46, Brussels 25/01/2012

[48] According to paragraph 3.2 of the Data Protection Regulation Proposal, "The EU is also best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries."

[49] Indeed, though the DPR allow users to claim their data protection right against cloud providers, it should be noted that certain legislation "might ultimately hinder the privacy and confidentiality of information for the sake of protecting national security and public order. This is the case of certain countries whose laws can oblige Cloud providers to communicate to the authorities any information that constitutes evidence of criminal activities". For instance, such a data protection limitation might be ascribed to the" USA PATRIOT Act, which entitles the FBI to compel - following a court order - the disclosure by U.S. Internet service providers of any record stored on their servers (50 U.S.C. § 1862)" See: De Filippi P. , McCarthy S. (2012) Cloud Computing: Centralization and Data Sovereignty, in European Journal of Law & Technology, August 2012

[50] According to the DPR proposal "When establishing technical standards and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interoperability and innovation".

With regard to net-neutrality, the situation is slightly more complex. On the one hand, non-discrimination obligations would preclude ISPs from charging Cloud providers more for acquiring priority access to the network. Ensuring that packets are always treated equally would facilitate the entrance of competing services in the market by reducing the potential new barrier to entry that new service providers would otherwise encounter *vis-à-vis* established providers. In addition, non-discrimination rules may encourage ISPs and network operators to undertake infrastructural investments aimed at improving the speed and quality of all Internet communications - whereas, allowing them to charge for priority access would actually constitute an incentive for them to keep the general quality of Internet connections low.

On the other hand, however, rules prohibiting any form of packet discrimination may be regarded as excessively draconian. Indeed, as previously illustrated, priority access to the network may be advantageous to both Cloud providers and users - who would be able to enjoy a faster and more reliable connection to specific online services. The implementation of *ex-ante* net neutrality rules would therefore ultimately require a nuanced approach, to preserve competition in the market while nonetheless allowing for the establishment of innovative business models within a competitive environment.

An alternative strategy would suggest adopting a more *laissez-faire* approach, letting the market mechanisms sort out the problem and only intervening *ex-post* through the tools provided under competition law - whenever it becomes evident that the market cannot autonomously restore competition. Such an approach would require a throughout investigation of the market for online services in order to establish the extent to which a single entity or group of entities actually dominate the market. Should dominance be found, barriers to entry should be assessed to determine whether or not they may preclude competition in the market. It should be noted that, in in the case of Cloud Computing, barriers to entry are already substantial for a variety of online services. Service providers, such as Google, Apple and Facebook, for instance, currently enjoy huge market shares and may be tempted to leverage their dominance into new markets.[51]

Yet, according to this approach, competition authorities should only intervene when evidence of an alleged abuse of dominance is found, or if a merger between two or more service providers would drastically jeopardize competition in the market.[52] Short of either of these two situations, governmental intervention would be unjustified, thereby delegating to the market the responsibility to solve

---

[51] See, for instance: Cave M., Williams, H., "The Perils of Dominance: Exploring the Economics of Search in the Information Society, March 2011.

[52] This principle has been at least acknowledge by the European Union. Indeed, according to Paragraph 5 of the Directive 2009/140/CE of the European Parliament and of the Council of 25 November 2009, "The aim is [...] ultimately, for electronic communications to be governed by competition law only". See: [2009] Official Journal of the European Union, L 337/37.

interoperability and data-portability issues, as well as to guarantee the protection of users' fundamental rights.

The position of this paper is that, aside from these two approaches, it would be perhaps more effective to look for alternative solutions to the aforementioned issues in the realm of private ordering.

An interesting solution is, for instance, Eben Moglen's *Freedom Box,*[53] intended to users back control over their own data. The Freedom Box is a small and cheap device which functions as a private server featuring built-in privacy and security settings. By shifting power and information away from corporate or governmental bodies, the Freedom Box can be regarded as a user-empowering mechanism aimed at protecting online privacy and ensuring data security. Another experimental solution is offered by the recent deployment of spontaneously organized wireless *mesh networks* - local area networks (LAN) that operate independently from the Internet infrastructure.[54] Indeed, the technical infrastructure of most mesh networks is created through the wireless capacities of users' devices (cellphones, WiFi routers, etc.) and operated as a peer-to-peer network - being every device simultaneously a node and an access provider for other nodes. This creates a flexible, dynamic and potentially resilient network, that operates independently from the terms and conditions of traditional ISPs in terms of access and bandwidth.

However, even if these technologies are publicly available to the general public, they are often technically complex to operate, therefore excluding a large section of users from using them. Besides, a plethora of data is currently being held - whether we like it or not - by governments and corporations with which we interact (e.g. banks, credit cards, or ISPs). To the extent that their data management might rely on online Cloud services, at present, a legal or regulatory approach cannot be completely discounted in favour of liberating technologies.

As a matter of fact, regulation could either aid or impede these technologies. While it might promote the development of innovative technologies, the law might as well preclude their deployment by excessively regulating the framework in which they operate. For instance, by encouraging unlicensed uses of the WiFi spectrum, the law can support the development of openly available wireless

---

[53] FreedomBox is a community project to develop, design and promote personal servers running free software for distributed social networking, email and audio/video communications.The project was announced by Eben Moglen at the New York ISOC meeting on February 2, 2010. See http://freedomboxfoundation.org

[54] See: Hassnaa M.et al. "A Panorama on Wireless Mesh Networks: Architectures, Applications and Technical Challenges", 2006; Akyildiz I.F., Wang X., Wang W., "Wireless Mesh Networks: A Survey" in Computer Networks – Elsevier Science no. 47, Jan. 2005; Bruno R., Conti M. and Gregori E., "Mesh Networks: Commodity Multihop Ad hoc Networks," in IEEE Communication Magazine, March 2005.

networks, encouraging further innovation in mobile communications. Conversely, proposals to regulate the WiFi spectrum would most likely annihilate any opportunity for the mesh network to subsist.[55] Similarly, while network neutrality may protect consumers in the short run, it might simultaneously diminish the need for the deployment of an alternative communication network - thus eventually harming the consumers in the long-run by discouraging the development of an innovative platform that the market would have otherwise provided. In the words of J. Schumpeter, in order to encourage the process of "creative destruction", it is sometimes better to let competition in the market die, in order for a new market to emerge.[56]

[55] For more information on WiFi spectrum management, see: Yochai Benkler, 2002, "Some Economics of Wireless Communications", Harvard Journal of Law & Technology, vol. 16.

[56] The term creative destruction (from German: schöpferische Zerstörung) is associated with Joseph Schumpeter, who used it to describe the disruptive process of transformation that accompanies innovation. For instance, in terms of technology, the vinyl was replaced by the tape, which was subsequently replaced by the compact disc, later replaced by MP3 players, which will in turn eventually be replaced by newer technologies.