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

Primavera de Filippi, Luca Belli

Law of the Cloud v Law of the Land:

Challenges and Opportunities for Innovation

Primavera De Filippi

Luca Belli

- CERSA / CNRS / Université Paris II -

Abstract:

Cloud Computing enables the dynamic provision of resources on-demand over the Internet. The key advantage for users is that data becomes accessible from anywhere and at any time. However, to the extent that they lose control over the infrastructure, users can no longer control the way data can be accessed by them or by others. This is likely to negatively affect the fundamental rights of end-users in terms of privacy and freedom of expression.

Assuming that market mechanisms alone are unable to preserve competition in the market for Cloud services, some other form of regulation might be necessary. This paper will compare the advantages and drawbacks of two types of governmental intervention (ex-ante regulation and ex-post regulation) to conclude that the law should ultimately encourage self-regulation by the market players themselves.

Keywords:

Cloud Computing, private ordering, innovation, privacy, freedom of expression, net neutrality.

Introduction

Cloud computing represents an innovative use of information and communication technologies which has drastically modified the way in which computing resources are used and deployed over the Internet. Hardware and software resources are delivered on demand through the Internet, eliminating the need for users to purchase expensive computers and/or software applications. Similarly, data need no longer be stored on users' devices; they can be exported in large data-centers where they can be easily processed by Cloud operators. Consequently, the decentralized structure of the Internet (built on the 'end-to-end' principle) is slowly being supplanted by increasingly large and centralized infrastructures (designed around the concept of 'mainframes').

The first section of this paper will analyse how this shift may affect the fundamental rights of users, mainly with regard to the right of privacy and freedom of expression. Indeed, given that they control most of the data passing through their platforms, Cloud providers have the ability to infringe users' rights - e.g. by collecting and/or processing personal data without authorisation, or arbitrarily censoring certain types of communication.
Theoretically, it could be assumed that, in a competitive market, market players will eventually be forced to adapt to users demands and expectations in order not to lose market share. Yet, the Cloud market is an oligopolistic market dominated by a few large corporations concerned with the maximization of their own profits. The second section of this paper will examine the behavior of these market players, and how they contribute to increasing or preserving their market share both by locking users into they systems and by claiming priority access to the network - without paying particular concern to the fact that their activities might impinge upon users' privacy and freedom of expression.

Finally, the last section will address the potential solution that may be endorsed in order to preserve the fundamental rights of users, without constraining innovation. After addressing the distinction between *ex-ante regulation* (e.g. through the definition of net neutrality rules) and *ex-post regulation* (e.g. by means of competition law, consumer protection law, etc.), the paper will assess their corresponding benefits and drawbacks so as to determine whether either of them, or a combination of the two, could successfully preserve users' right without excessively limiting the operations of Cloud providers. Finally, the paper will explore the viability of alternative forms of regulation based on *self-regulation* and *technical regulation* by end-users. Indeed, users are becoming increasingly aware of the risks derived from Cloud computing, and are developing specific technologies and software applications in order to counteract the negative effects that certain Cloud services might have on their fundamental rights.

Rules are, consequently, no longer dictated by Cloud operators in a *top-down* fashion; they are, instead, established by the users themselves through a *bottom-up* approach.

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 - or software resources - such as platforms and applications. 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 webmails, web-based document storage, as well as many web-based production and collaboration tools.

Cloud computing can be distinguished into different types and categories according to the nature of the resources they are concerned with (Infrastructure as a Service,[3] Platform as a Service,[4] or Software as a service[5]), and the extent to which they are being deployed (e.g. public, private, hybrid and community clouds). Different deployment models will have a different impact on users' right to privacy, data protection and freedom of expression. Given their potential effect on these fundamental rights, we will refer - for the purpose of this paper - almost exclusively to Cloud computing technologies deployed as a public Cloud in the form of Software as a Service.

From the perspective of end-users, the main advantage of this type of Cloud Computing is that data become a resource accessible from anywhere and at any time, as long as there is an

---

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." See: Peter Mell and Timothy Grace, The NIST Definition of Cloud Computing. National Institute of Standards and Technology, NIST Special Publication 800-145, 2009, available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (last visited October 5th 2012

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) is more complex form of Cloud Computing, which provide users with a computing platform -typically including an operating system, a programming environment, a web server and a variety of databases.

5 SaaS (Software as a Service) is a specific type of Cloud Computing that provides an interface to computer software or other online application that do no longer need to be run on the end-users devices.

Internet 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 used or accessed 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 most of the data stored in the Cloud.

At present, the distributed and decentralized architecture of the Internet is increasingly threatened by the centralised processing and storage of data undertaken by many Cloud operators - which have acquired considerable power with regard to what may or may not be done with the information they hold. Private ordering allows Cloud providers to impose their own rules onto users, both contractually - by means of specific Terms of Service - and technically - through the actual infrastructure of the Cloud. Oftentimes, the lack of bargaining power on the side of the users is such as to give them no other choice than accepting the rules dictated by the cloud providers (or abstaining from the use of their services).
Besides, the transnational character of Cloud computing, combined with the opacity of its operations, is such that users generally have no control or knowledge over the exact location of data.[6] A number of challenges must therefore be addressed to determine the applicable law and the extent to which users' rights will be effectively protected. The following sections will focus on how centralised infrastructures might negatively affect the fundamental rights of users - endangering their privacy and potentially jeopardizing their freedom of expression.

A. Privacy, data protection and confidential information

Cloud computing triggers the application of several regulations that enshrine different conception of privacy and data protection, and different degrees of protection for confidential information. Hence, Cloud computing could have serious implications on the privacy of personal information and on the confidentiality of corporate or governmental information.[7]

6 See: Peter Mell and Timothy Grace, op. cit. p. 2.

7 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

To begin with, it should be recalled that, at the European level, privacy and data protection are perceived as fundamental rights[8] that deserve *erga omnes* protection[9]. Indeed, the judicial tradition of many European countries have delineated privacy as an attribute of person-hood that cannot be waived and that should be protected against all.[10] Such a perception has led to reaffirm, on a regional level, the fundamental right to respect for one's private and family life, home and communications - which has been endorsed by both article 8 of the European Convention on Human Rights and article 7 of the European Charter of Fundamental Rights - and the fundamental right to the protection of personal data - which is specifically enshrined in article 8 of the Charter.

Conversely, in the United States (where the majority of Cloud providers' headquarters are located), the Constitution contains no express right to privacy. The American conception of privacy fundamentally coincides with the "right to be left alone"[11] - a right whose constitutional basis can be found in the Fourth and Fifth Amendments of the Bill of Rights.[12] Indeed, as it has been remarked by James Withman, the conceptual core of the

---

8 See: Article 7 and 8 of the Charter of Fundamental Rights of the European Union, which respectively enshrine the Right to respect for private and family life (privacy right) and the right to the protection of personal data (data protection). The protection of personal data is also protected by Article 17 of the Treaty on the Functioning of the European Union, and has been further corroborated through the European Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (currently under revision).

9 As Hon. Mr. Justice John L. Murray has remarked, "EU law is characterized by the principles of direct effect and primacy of Community law in relation to national law, and thus forms an integral part of national law in each member state, which is relied upon and enforced by national courts. Thus, EU law and the decisions of the Court of Justice may be relied upon by individuals before national courts in all Member States. The ability to do so applies in a uniform manner in all Member States and is not dependant on, or governed by, national legislation. Reflecting the high degree of integration at the EU level, the decisions of the Court of Justice have a direct impact on domestic legal systems as they are binding *erga omnes*, and strong mechanisms exist for their enforcement". See: John L. Murray, The Influence of the European Convention on Fundamental Rights on Community Law, Fordham International Law Journal, Vol 33, Issue 5, 2011, p. 1391.

10 See: James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, The Yale Law Journal, Vol. 113, 2004. See also: François Rigaux, L'individu, sujet ou objet de la société de l'information, Groupe d'études Société d'information et vie privée, 2008.

11 See Olmstead v. United States, 277 U.S. 438, 471-85 (1928) (Brandeis, J., dissenting): "The makers of our Constitution understood the need to secure conditions favorable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality -- *the right to be left alone* -- the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect."

12 Such an interpretation of the Fourth Amendment has been formulated by Samuel Warren and Louis Brendis famous article and reiterated by Louis Brandis himself in his famous dissenting opinion in Olmstead v. U.S. Warren and Brandeis indeed argued that "[t]he makers of our Constitution sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment" See: Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193(1890)).

American right to privacy "still takes much the form that it took in the eighteenth century: it is the right to freedom from intrusions by the state, especially in one's own home."[13] Unlike the situation in Europe, therefore, privacy in the U.S. (as a constitutional right) has been tailored to be exclusively asserted against the State - even though specific statutory laws have subsequently endorsed a legal right to privacy enforceable also against the private sector by means of a "sectoral approach".[14]
This distinction is of particular relevance because Cloud computing generally relies upon the activities of a plurality of stakeholders operating from different jurisdictions - all contributing to the provision of a single Cloud service. Hence, in the lack of agreed provisions to determine the applicable law for any given Cloud service, each stakeholder involved will remain subject to its own national legislation. This is likely to lead to a concurrence of different national laws[15] - frequently involving U.S. legislation.

As a general rule, in the context of Cloud computing, the rights to privacy and data protection are affected only to the extent that users might disclose information which qualifies as "personal data" - the processing[16] of which is framed by a number of legal provisions.[17]

---

13 See: James Q. Whitman, op. cit., p. 1163

14 Starting from the 1970s, legislation has been enacted to introduce privacy protection with regard to specific sectors of activities. The first amongst these pieces of legislation was the Fair Credit Reporting Act, which was enacted in 1970 to promote accuracy, fairness, and the privacy of personal information assembled by Credit Reporting Agencies. For further details, see: EPIC, The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report. Another example of the U.S. sectoral approach to privacy may be found in the Health Insurance Portability and Accountability Act (1996), which has introduced a right to information privacy in the health sector. With regard to the online environment, it should be noted that specific protection has been accorded to the privacy of children under the age of 13. Indeed, the Children's Online Privacy Protection Act (COPPA) - which took effect in 2000 - has been specifically tailored to protect the privacy of children by requesting parental consent for the collection or use of any personal information of the users. See: EPIC, Children's Online Privacy Protection Act (COPPA).

15 It is worth to underline that this heterogeneity of applicable laws involves also the juridical systems within the European Union. Indeed although the Directive 95/46/EC has provided a certain degree of harmonization, the Member states have elaborated 27 slightly different approaches in order to integrate the directive to their national systems. Notably, discrepancies may be found with regard to approaches adopted to frame financial data, health data, etc. It is indeed by reason of this fragmentation that the European Commission has suggested the adoption of a Regulation – which is a directly applicable juridical tool – amongst the juridical tools aimed at redefining in a uniform fashion the legal framework of the personal data protection.

16 Under Article 2(b) of Directive 95/46/EC "*'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*".

17 Directive 95/46/EC has set forth some specific duties and obligations on the "data controller" and the "data processor". Under Article 2 of the Directive, "*(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; [...](d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; (e) 'processor' shall mean a natural or legal person, public authority,*

In this respect, it should be noted that Cloud operators can gather a considerable amount of information about their users - which can be disclosed either explicitly or implicitly through their actions. As regards personal data, while they are often disclosed directly by users (e.g. in the process of subscribing to the service), they might also be revealed unwillingly to the Cloud operator - who can subsequently exploit this information to its own benefit.[18]
The rights to privacy and data protection are thus likely to be violated by a variety of Cloud operators[19] that process personal data beyond what is strictly necessary to provide a service to their user-base, often with a view to create personalised profiles delineating the habits of the user-base. User profiling has indeed become an extremely lucrative tool to provide customised and targeted advertisements. Yet, as we will explain later, these profiles may eventually be disclosed to third parties or accessed by foreign agencies - thereby further endangering the privacy of users.

These issues are further complicated by the fact that, in order to improve the speed and reliability of Cloud services, data is frequently copied and processed on several servers at the same time. Jurisdictional issues may arise insofar as these different data centers are located in different countries with divergent privacy standards. As it has been highlighted by Peter Hustinx (European Data Protection Supervisor): only Cloud operators established in the EU and/or using equipment in an EU Member State (or acting as a processor for a controller using such equipment) will in principle be 'caught' by EU law; others will escape EU law - even if they mainly and mostly targets European citizens.[20]
Therefore, in order to protect the fundamental right to privacy of European citizens, Directive 95/46/EC precludes the transfers of personal data to any third country that does not provide an adequate level of protection[21] as regards the processing of personal data. In

---

agency or any other body which processes personal data on behalf of the controller". Duties and obligations are specified in article 6, 7, 10, 12, 17, 25, 26.

18 As an example, one may think about the Facebook like button which besides allowing Facebook users to share the content they like with their "friends", places "cookies" on the user's browser, in order to "recognise" the user and eventually track its browsing habits. The very purpose of the pieces of software named cookies is indeed to recognise a specific user and trace his browsing habits. Indeed, every time that the user will visit a webpage containing a like button, the cookies will will make him recognisable. To this latter extent, see as an instance A.P.C. Roosendaal, "We Are All Connected to Facebook…by Facebook!", in: S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?*, Heidelberg: Springer (2012), pp. 3-19.

19 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.

20 See: Peter Hustinx "Data Protection and Cloud Computing under EU law", Third European Cyber Security Awareness Day,Panel IV: Privacy and Cloud Computing, BSA, European Parliament, 13 April 20, p. 3.

21 According to the European Commission, the following countries are deemed as providing 'adequate' data protection standards: Andorra, Argentina, Australia, Canada, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, Switzerland, Uruguay and the US, thanks to the Safe Harbor Agreement. Indeed, the Council and the European Parliament may give the Commission the power to determine, on the basis of Article 25(6) of directive 95/46/EC, "whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into". The adoption of a - comitology - Commission decision is based on Article 25.6 of the Directive. See: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

this respect, the US approach to privacy - as a combination of sectoral laws and self-regulation[22] - can hardly be regarded as an adequate standard from an European perspective. Yet, the gap between the protection granted in the EU and in the US has been bridged by the US-EU Safe Harbor Agreement,[23] meant to safeguard the free flow of information between the US and the EU[24] by establishing a voluntary mechanism that allows US organizations to self-certify their adherence to a particular set of Privacy Principles deemed as a sufficient level of privacy protection.

The confidentiality of information[25] 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.[26]

Indeed, in certain jurisdictions information stored in the Cloud may be accessible by governmental agencies, in spite of the rights and protections guaranteed under the user's domestic law.[27] For instance, Section 217 of the US Patriot Act allows US governmental agencies to intercept the communications of any "computer trespasser" as long as they have obtained authorization from the "owner of a protected computer" - an entity that could potentially qualify as a service provider.[28] The Patriot Act thereby exonerates the US government from the need of obtaining a warrant to intercept online communications.

---

22 See: Ira S. Rubinstein, Privacy, Self-regulation and statutory safe harbors, p. 14, available on http://www.ftc.gov/os/comments/privacyroundtable/544506-00022.pdf (last visited October 4th 2012

23 The Safe Harbor Agreement has been jointly developed by the US Department of Commerce and the European Commission and has been approved through Commission Decision 2000/520/EC.

24 The importance of preventing the interruptions in international flows of data has been recognised as a predominant issues since the adoption in 1980, of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.according to which "*[r]estrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance*". See: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, available at http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited October 5th 2012)

25 Confidentiality should be considered as the preservation of "authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information". See: Directorate General for Internal Policies, Cloud Computing, Study, May 2012, p. 7.

26 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

27 E.g. 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"

28 Indeed, the provided definition of "protected computer" is particularly broad insomuch as being quasi-omnicomprehensive, encompassing also the systems "used in interstate or foreign commerce or communication".

Furthermore, data confidentiality can be threatened by exporting data into centralized Cloud infrastructures, insofar as the user loses control over that data.[29] In particular, it should be noted that, in the US, the "business record doctrine" (or "third party doctrine") stipulates that confidential information is no longer protected by the Fourth Amendment when it is knowingly revealed to a third party - since disclosure implies relinquishing control over information.[30] Anyone communicating private information to a third party Cloud operator should therefore assume that such information can no longer be reasonably considered as private or confidential.

Finally, 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 higher - and the impact much greater - in the context of Cloud computing.[31] On the one hand, users run the risk that data may be intercepted during their transmission to the Cloud. On the other hand, data stored in the Cloud could either be *deliberately* disclosed to unauthorised parties by the Cloud operator itself (e.g. under an expectation of remuneration) or be *accidentally* made available to third parties (as a result of a fault or security breach). Hence, in order to preserve users privacy and confidentiality, Cloud operators need not only comply with data protection regulation, but also adhere to specific duties of care and incur the infrastructural costs necessary to guarantee the security and integrity of online communications.[32]

B. Freedom of expression

Freedom of expression is a fundamental right, enshrined, *inter alia,* in the International Covenant on Civil and Political Rights (article 19), and the European Convention on Human Rights (article 10). Yet, freedom of expression shall not be conceived in absolute terms. While it has been recognized as a fundamental right by most international treaties and conventions, the right to freedom of expression (or free speech) is subject to a number of limitations bent on preserving particularly relevant interests - such as public order, morality, national security and public health. To this extent, national legislators have been allowed to incorporate into the law a limited series of exception to the enjoyment of this right.

---

29 See: Directorate General for Internal Policies, Cloud Computing, Study, May 2012, p. 45.

30 See: Orin S. Kerr, The Case for the Third-Party Doctrine, Michigan Law Review, Vol. 107, 2009. See also: *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976) according to which: "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."

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

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

Freedom of expression might, however, be significantly challenged by Cloud computing in a way that extends way beyond these exceptions. Indeed, since all communications passing through the Cloud can theoretically be monitored by the infrastructure provider[33] (unless these have been encrypted beforehand), they can potentially be filtered and/or censored by the various Cloud operators involved in the transmission thereof.
For instance, Facebook's Terms of Service prohibits "obscene" and "sexually explicit" material[34] - where the assessment of such material is unilaterally carried out by Facebook's staff itself.[35] Hence, when the social network decided to ban pictures illustrating naked breasts, many mothers had their breast-feeding pictures removed from their Facebook profiles without any opportunity of challenging this decision.[36] 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 user interface can produce normative governing effects similar to laws. However, as opposed to the *Law of the Land*,[37] which must necessarily be enforced by public authorities, the *Law of the Cloud* can be automatically enforced by the technical functionalities provided by the platform – which can

---

33 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. B.H. Takabi, Security and Privacy Challenges in Cloud Computing Environments, Security and Privacy, IEEE, Volume 8, Issue 6, Nov-Dec 2010

34 See: Facebook Terms of Service, available at http://www.facebook.com/legal/terms (last visited, October 4th 2012).

35 See, for instance, Facebook's unilateral decision to remove pictures of breastfeeding women which were considered as obscene (in February 2012) and Facebook's decision to block the accounts of several women members of a Brazilian activist group called "*Marcha das Vadias*" – which is Brazilian for "Slut's walk" – because they posted pictures portraying them protesting with uncovered breasts (in May 2012), see: http://www.telegraph.co.uk/technology/facebook/9072201/Why-lactivists-are-milking-Facebooks-breastfeeding-ban.html and http://www1.folha.uol.com.br/tec/1097488-facebook-bloqueia-usuarias-que-aparecem-seminuas-em-fotos-da-marcha-das-vadias.shtml (last visited, October 4th 2012)

36 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, last visited June 25th 2012.

37 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*[...]"

be used either to enhance or to impede basic freedoms. If it is true that, as stated by Lawrence Lessig, "Code is law"[38], 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.[39] If the "medium is the message",[40] 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.[41] 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.[42]

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.[43] In a competitive market, a service provider that does not respect the expectations of

---

38 Lessig L., Code: And the Other Laws of Cyberspace, Version 2.0, 2006.

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

40 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.

41 According to the US 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).

42 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

43 A liberal approach to market economics assumes that "the marketplace will protect privacy because the fair treatment of personal information is valuable to consumers; in other words, industry will seek to protect personal information in order to gain consumer confidence and maximize profits. For more than twenty years,

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.[44] 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.[45]

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.

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,[46] and was reiterated in 2004 by the Court of First Instance which

---

however, government agency task forces and reports regularly illustrated the lack of fair information practices in American society, but nevertheless resorted to the mantra that business should be given more time to self-regulate". See: Joel R. REIDENBERG, Restoring Americans' Privacy in Electronic Commerce, 14 Berkeley Tech. L.J. 771, 774, 1999; Peter P. Swire, Markets, Self-Regulation, and Government Enforcment in the Protection of Personal Information, in U.S. DEPT. OF COMMERCE, NAT'L TELECOMM. AND INFO. ADM., PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE, June 12, 1997.

44 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.

45 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"

46 In the IBM case, Article 86 (now Art. 102 TFUE) infringement proceedings were brought against IBM by the European Commission. 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.

confirmed an infringement decision against Microsoft for failing to supply interoperability information to its competitor.[47] In addition, by virtue of the *Intel/McAfee* case, interoperability – notably, "degradation of interoperability" – gained a prevalent role in EU decisional practice.[48] 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.[49]

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 behaviours.[50] Thus, in order to ensure that consumers can freely chose and switch across the most competitive services, data portability - and, eventually, 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 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.[51]
Such behaviour has recently been ascribed to Google by virtue of its AdWords search advertising platform and AdWords Application Programming Interface (API).[52] 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

---

47 See: Case T-201/04, *Microsoft Corp. v. Commission of the European Communities*, Judgment of the Court of First Instance (Grand Chamber), 17 September 2007.

48 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

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

50 See, in particular, Case T-201/04 *Microsoft Corp. v. Commission of the European Communities*, ECR II-4463

51 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

52 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.

introduced a considerable barrier to the utilisation of any competitive platform.[53] This affair illustrates how interoperability limitations can be used to trigger unnatural network externalities,[54] 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.[55] 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.

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. Positive externalities are created as new users increase the actual value of the service they use. 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 Computing, 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.*[56]

---

53 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.

54 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.

55 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.

56 The bandwagon effect - also known as the copycat behaviour - 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' behaviour. This situation may impair competition in the market, potentially leading to a situation of monopoly where "the winner takes it all."

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 keeps 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[57] - 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.

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.[58]
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).[59] While it has been strongly criticized by net neutrality advocates,[60] data discrimination might actually bring a series of benefits to users eager to enjoy higher quality services on the Internet. Indeed, users may find 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

---

57 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.

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

59 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.

60 See, for instance: La Quadrature du Net, "Protecting Net Neutrality in Europe", 2009

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*"[61].

In the context of Cloud Computing, in order to cope with the considerable augmentation of bandwidth consumption determined by online services – particularly with regard to audiovisual applications[62] – 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 behaviours 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.[63] 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[64] while elaborating the Telecoms Package.[65] Although the principle of net neutrality has not been fully endorsed by

---

61 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.

62 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.

63 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.

64 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

65 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.

European legislation, it has nonetheless been recognized as a useful means to promote competition and transparency in the 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[66] and to impose transparency obligations for network operators[67] 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 analyse 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.

---

66 See : Recital 34 and Article 22(3) of the Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

67 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,[68] 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:[69] electronic communications regulation (cf. the Telecoms Package), electronic commerce regulation (cf. the Electronic Commerce Directive)[70] 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. Market mechanisms are thus likely to lead towards the centralization of resources, with a consequent loss of user control. As a result, the market for Cloud Computing services is likely to be dominated by a few very large players, which may be tempted to abuse their dominant position in the market - a situation which might result in adverse effects on the right to privacy, data protection and freedom of expression.

Assuming that, once a certain number of dominant players are 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 choose the service that best satisfies their needs.
The fundamental question that will be addressed in the following sections is whether competition should be preserved through *ex-ante* or *ex-post* regulation. *Ex-ante* regulation would require broader enforcement of fundamental rights and/or the introduction of strong net neutrality rules (e.g. in the form of non-discrimination obligations), whereas ex-post regulation would essentially rely on the judiciary tools which are already available under competition law or other bodies of law (such as data protection and consumer protection laws). To conclude, the paper will investigate whether it might be possible to resolve these problems by resorting exclusively to market-based regulatory strategies, i.e. self-regulation by the market actors and users themselves.

A. *Ex-ante* regulation

68 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

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

70 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

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. This has led to the development of a new data protection framework provided by the recently proposed Data Protection Regulation (DPR).[71] 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),[72] 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.[73]

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.[74] 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.

With regard to net-neutrality, the situation is slightly more complex, since enforcing net neutrality through regulation might lead to two contrasting results.

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-*

---

71 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

72 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."

73 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 US 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

74 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".

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.

B. *Ex-post* regulation

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 would then 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.[75] 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.[76] Short of either of these two situations, governmental intervention would be unjustified, thereby delegating to the market the responsibility to solve interoperability and data-portability issues, as well as to guarantee the protection of users' fundamental rights.

---

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

76 This principle has been at least acknowledged 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.

C. Self-regulation

The position of this paper is that, aside from these two approaches, it would be perhaps more effective to look for alternative solutions to market failure. If the aforementioned issues cannot be properly solved neither by ex-ante nor by ex-post regulation, it is worth exploring whether it might be possible to address them through a different approach based on self-regulation by private parties.

Self-regulation[77] implies a certain degree of independence from State regulation, as market players regulate themselves - developing common rules and self-enforcing them. In the context of Cloud computing, self-regulation might be adopted in order to increase professional reputation and preserve ethical standards. This can be achieved, for instance, by promoting certain practices (interoperability, privacy-compliant services, etc.) and banning others types of activities that might negatively affect the user-base (user-profiling, targeted advertising, arbitrary censorship, etc).

Yet, given the characteristics of the market for Cloud services (dominated by few large corporations), private regulation amongst market players is unlikely to lead to satisfactory results. The State might therefore intervene in order to push self-regulation in the right direction. Indeed, although self-regulation only concerns a limited number of market players, to the extent that they operate within the boundary of the State, they are nonetheless subject to national rules. State regulation can create the necessary infrastructure and provide the necessary incentives for Cloud providers to regulate themselves in a way that properly takes into account users' demands and expectations.

However, self-regulation is not only limited to the realm of market players; it could be - and has already been - implemented amongst specific communities of users eager to autonomously establish the rules to which they will have to abide, rather than complying to the rules dictated by third party Cloud operators. This particular type of self-regulation distinguishes itself from the self-regulation of Cloud operators insofar as it does not primary rely on standard agreements or codes of conducts, but rather on technical means (hardware or software) developed by users to address what has not been properly provided by Cloud operators. These tools are designed to provide users with a means to delineate their preferences in a series of rules that are automatically enforced through technological means, regardless of whether or not they comply with the policy of various Cloud operators. These rules can thus be regarded as some form of private ordering achieved through *bottom-up technical regulation*.

To this latter extent, an interesting example is Eben Moglen's *Freedom Box,*[78] intended to give 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

---

77 The 2003 Inter-institutional Agreement on Better Lawmaking defines self-regulation as "the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines [...] (particularly codes of practice or sectoral agreements)".

78 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

and information away from corporate or governmental bodies, this device endow users with complete control not only over their data, but also over the infrastructure of communication, thereby protecting online privacy and promoting freedom of expression. While it actually operates outside of the Cloud computing framework, the Freedom Box has nonetheless an impact on the Cloud market to the extent that it constitutes an alternative and competitive service that provides ubiquitous access to data stored and processed in a private device - without impinging upon user's rights. As such, the Freedom Box can be said to exert an indirect effect over the practices of Cloud operators, which can no longer abuse their power without incurring the risk of losing at least part of their user-base.

Another answer to market failure - mostly as a response to the growing concerns for net neutrality - is illustrated by the recent deployment of spontaneously organized wireless *mesh networks* - local area networks (LAN) that operate independently from the Internet infrastructure.[79] Indeed, the technical infrastructure of most mesh networks is created through the wireless capacities of users' devices (mobile phones, 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. Although still at an experimental stage, were it to be more widely deployed, the mesh network could potentially represent a viable alternative to the Internet network, which might seriously affect - albeit indirectly - the operations of many Internet service providers.

The problem is that, 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 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.[80] 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

---

79 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.

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

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.[81]

81 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.