HAL
open science

Ubiquitous Computing in the Cloud: User Empowerment vs. User Obsequity

Primavera de Filippi

To cite this version:

Primavera de Filippi. Ubiquitous Computing in the Cloud: User Empowerment vs. User Obsequity. User Behavior in Ubiquitous Online Environments, IGI Global, pp.44, 2013. hal-00855712

HAL Id: hal-00855712

https://hal.science/hal-00855712v1

Submitted on 2 Sep 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Ubiquitous Computing in the Cloud: User Empowerment -vs- User Obsequity.

Primavera De Filippi1
CERSA / CNRS / Université Paris II, France

ABSTRACT

This paper analyses the evolution of the Internet, shifting from a decentralized architecture designed around the end-to-end principle with powerful mainframe/personal computers at each end, to a more centralized network designed according to the mainframe model, with increasingly weaker user's devices that no longer have the ability to run a server nor to process any consistent amount of data or information. The advantages of ubiquitous computing (allowing data to become available from anywhere and at any time, regardless of the device) should thus be counterbalanced with the costs it entails (loss of users' autonomy, concerns as regards privacy and freedom of expression, etc).

INTRODUCTION

The advent of Internet and digital technology drastically changed the way people act and interact in everyday's life, in both personal and professional settings. Indeed, with the Internet, work, family and social life are becoming increasingly intertwined, sometimes even blurring into each other. The office does not longer consist exclusively of a place for work, but is increasingly used by people dealing with personal matters, via e-mails, instant messaging or social media. Conversely, professional activities extend throughout the day - either at home or at the office during lunch break, while traveling, or in the evening after a long day of work, people do not hesitate to check their e-mails and, if necessary, to complete their work. This naturally implies that people must be able to access their personal or professional files from anywhere and at any time, without direct access to their computer. Thus, in most developed countries, the Internet has become a necessity.

Ubiquitous computing is an attempt to answer emerging users' need for ubiquity. Without trying to resolve any specific business or technical problem, it represents an effort to elaborate new opportunities based on pervasive computing and connectivity (Bell & Dourish, 2007).

Nowadays, computing has become an integral part of everyday life - yet, it is much less visible than before. Technological advances in the computing industry are such that electronic devices can be embedded in the environment in a way that is almost transparent to end-users (Weiser, 1991). Recent developments in information and communication technologies (ICT) encouraged the deployment of compact users devices that communicate with powerful servers and distributed data-centers in order to mediate and support many daily activities (Lyytinen & Yoo, 2002). Personal computers, laptops, tablets or even mobile phones are turned into "intelligent devices" able to provide innovative services and applications to satisfy emerging users' needs in ways that could hardly be foreseen even just a few years earlier. Indeed, thanks to the Internet, any device - with limited computing resources - can potentially provide access to a world of information that was previously only available to a limited number of people connected to a given network.

This chapter analyzes the social, technical and legal implications of ubiquitous computing in the framework of cloud computing - distributed network architectures designed to provide computing resources as a service. After providing analysing the pro and cons of these new technologies, the chapter will address the implications that cloud computing might have on the interests of Internet users, whose autonomy is being increasingly impaired by the regulatory policy of large cloud operators.

[1] The author would like to thank David Lametti, associate professor at the Faculty of Law at McGill University, whose contribution has been extremely valuable during the drafting of this paper.

BACKGROUND

A. Definition of Cloud Computing

Cloud computing constitutes a new delivery model for IT resources based on the concept of utility computing - a model whereby computing resources are no longer sold as a product, but rather provided to consumers as a service. Although the term is nowadays used to refer to a large variety of online platforms, regardless of their technical attributes (Plummer & al., 2008), cloud computing specifically refers to distributed online platforms that provides configurable computing resources, dynamically, according to actual needs (Vaquero & al., 2008). The National Institute for Standards and Technology (NIST) defines cloud computing as any online platform that relies on ubiquity (broad network access), virtualisation (resource pooling), scalability and elasticity (automatic reconfiguration of resources) to provide on-demand (user-centric) metered services (pay-as-you-go).2

Depending on the type of resources they provide, cloud computing platforms can be subdivided into three distinct categories: Infrastructure as a Service (IaaS) is a model whereby hardware resources (such as processing power, storage capacity, or network bandwidth) are provided for consumers to decide how to best put them to us; Platform as a Service (PaaS) is a model whereby users are provided with a specific framework or programming interface on which they can deploy their own applications; whereas Software as a Service (SaaS) is a model whereby consumers are only given the possibility to use particular software or online applications through an online interface which is generally accessible through a web browser.

While cloud computing technologies are designed to allow users to access their resources from anywhere and at anytime, the actual degree of accessibility ultimately depends on type of cloud that one refers to. Namely, it is useful to distinguish between four different deployment models: public clouds, which are generally operated by one specific organisation that makes the infrastructure or the services it provides available to the general public, private clouds which are generally meant solely for the purpose of providing an infrastructure or a service to one specific organisation; community clouds which are intended to provide an infrastructure or services shared amongst several organisations that share similar goals or concerns, and, finally, hybrid clouds which combine two or more clouds (be them public, private or community clouds) into an aggregated structure.

For the purposes of this paper, we are mainly concerned with the impact of cloud computing on the online behaviour of users - whose interests are the most likely to be affected (both positively and negatively) by the latter category of clouds services. Throughout the paper, we will thus allude to cloud computing as referring to public clouds providing Software as a Service.

B. The opportunities of the cloud

More and more users are brought to interact with the cloud during their everyday life, in new and dynamic ways. Computing resources such as processing power, online storage and network bandwidth are progressively turning into a commodity which has become essential to most (Buyya & al., 2008). Yet, just like water, gas, electricity and telephony, computing resources no longer needs to be purchased by the users needing them, they can now be consumed (and paid for) on a daily basis according to actual needs (Banerjee & al., 2011). Users can thus immensely benefit from cloud computing technologies. Advantages relate not only to the benefits derived from the growing accessibility and flexibility of resources - including the comfort derived from their ubiquitous availability and ease of use, but also to the

[2] According to the National Institute for Standards and Technology (NIST), cloud computing is "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*." (Mell & Grance 2011)

new opportunities for anyone to experiment with new business models and to provide innovative services and applications without having to undertake any substantial investment beforehand.
Indeed, cloud computing technologies, based on virtualisation, enable users to acquire only the resources they need: this is the principle of the electric grid, where users only pay for the amount of resources they effectively use (Foster & al., 2008). This allows for a larger degree of flexibility in terms of both access and use. Given the ubiquitous character of cloud computing, in fact, data exported in the cloud become immediately accessible from anywhere and at any time, regardless of the user's device. The cloud also enhance and facilitate the deployment of these resources, by allowing users to employ sophisticated applications without having to install or configure them onto their own devices.
Besides, with the advent of cloud computing, new business opportunities have emerged online - attracting a large number of users and start-ups, experimenting with new business models without the need to plan ahead for provisioning (Zhang & al., 2010). This led to the emergence of a new value network operated by innovative market players that do not abide to the traditional value chain of service provision (Leimeister & al., 2010). Thus, the cloud industry eventually paved the way for the establishment of a new commercial paradigm (so-called u-commerce) extending traditional commerce to an environment characterised by network ubiquity, universality, uniqueness, and unison (Watson & al., 2002) through a series of online applications that users can access from anywhere and at anytime to enjoy unique and personalised services (Junglas & Watson, 2003).

C. The dangers of the cloud

These opportunities comes, however, at a potential cost. As user interaction with the cloud increases in both frequency and intensity, individuals also become much more vulnerable to it. Such vulnerability can be largely classed into two sets of concerns. The first category revolves around users' freedoms and the potential consequences of the cloud to users' fundamental rights. The second category revolves around the increased users' dependency on the structure of the cloud itself, and the potential disempowerment that might derive from the the manner in which users interact with it.
The cloud as an online repository of computing resources posits great challenges for the maintenance and respect of users' fundamental rights. In terms of freedom of speech, the potential exists for cloud providers to access, monitor, censor, filter, block and otherwise control communications on the internet (Karhula, 2010; Gervais, 2012; Ramachadran et al, 2011; Lessig 1997; Kshetri, 2010). Coupled with the general attitude of many users that do not hesitate to export personal information on the cloud, this makes for a great deal of personal data placed under the control of cloud-based service providers beyond the reach of users. Moreover, legal structures – contracts and copyright in particular – contribute to weakening users' ability to access information that should be freely available to all (De Filippi & Vieira, 2013).
The potential for user disempowerment (or *user obsequity*) is facilitated by the structure of the cloud itself. The internet began – indeed was deliberately conceived – as a decentralized network with few control points and designed around the end-to-end principle (Frischmann, 2012). Robust interaction with the Internet infrastructure mainly due to the open character of the network, and to the fact that users were, for the most part, connected through relatively powerful computing devices (Zittrain, 2008; Lametti, 2012). The emerging cloud architecture manifests a more centralized hierarchical structure, which, along with users interacting with less powerful devices (such as tablets or smartphone), allows for a much greater degree of control from the part of cloud service providers. As opposed to their former role of contributors to the network, under the cloud paradigm, user become passive service takers.

MAIN FOCUS OF THE CHAPTER

Issues, Controversies, Problems

A. From "smart phones" to "dumb-terminals" : the end of the end-to-end principle

The original infrastructure of the Internet was designed around the end-to-end principle and essentially made up of intelligent terminals that communicate with each other through the network. Fidelity to the decentralized architecture of the Internet was vastly assisted by the nonhierarchical, if not almost anarchical, structure of the network - which expands as users continually add to it (Lessig, 2006). Given the open-ended protocols upon which the network was created, the intelligence or intellectual drive of the Internet was originally highly diffuse and decentralized, yet anchored in individual users from around the globe contributing to the infrastructure by either providing their own computing resources or generating new content through individual computer devices.

Over the past 20 years, users have become more and more demanding: they constantly expect new services and innovative applications that cannot be easily provided on the limited architecture of most mobile devices. Most of these applications are thus increasingly provided on remote servers accessible through the Internet. Hence, with the advent of cloud computing, we are progressively moving away from the original structure of the Internet - based on a horizontal and decentralized architecture - towards a more verticalized and centralized architecture based on increasingly less sophisticated terminals communicating through centralized online applications. On the one hand, cloud operators are creating a series of centralized platforms by aggregating an humongous amount of computing resources into large data centers distributed around the world. On the other hand, users' devices are devolving from personal computers and laptops, to less relatively powerful tablets, smart-phones or any other device whose sole function is to access a particular online application - the so-called "thin clients" (Zittrain, 2009). Thus, as the opportunities of ubiquitous computing are drawing users away from the decentralized architecture of the Internet and up onto the cloud, network intelligence is progressively moving from the terminals to the core of the network, with the risk of bringing the end-to-end principle of the Internet to an end.

In this regard, it is useful to analyse the implications of the use of thin client devices on the way users interact and communicate according to at least four intertwined aspects: (a) the devices themselves, (b) the software they employ, (c) the services provided on these devices, and (d) the greater system into which they connect.

To begin with, while thin clients are certainly powerful compared to older desktops and laptops, they are relatively less powerful compared to other component parts of the current system. Indeed, most of these devices are simply not meant to do general purpose computing, they are merely meant to connect, through the Internet, to a centralized server on which all user data is stored and most of the processing is performed. The technological platform is no longer part of the device, but is ultimately dictated by the cloud provider.

Besides, as opposed to the open Internet, where users can chose the software they use as long as they comply with the protocol, users of these thin clients are often forced to be running the software applications dictated or sanctioned by specific (often proprietary) systems. As such, thin client devices are an effective means of restricting users to only those functions deemed appropriate or necessary by the cloud operator. Indeed, average users are generally unable to write new applications or add any other kind of functionality to enhance their devices, as such addition can only be accomplished with great difficulty. As they cannot easily get access to the underlying software or code of their own devices, and given that the software is not meant to be directly altered by them, users can only rely on the capacities of the device as determined (either at the outset or through a series of remote patches and continuous updates) by the

device or service provider (Zittrain,1990). No doubt, users are generally more concerned with the user interface than with the programming potential of their devices. Thus, although internally complex, these devices are programmed to be as simple as possible, user interaction with the device is conceived to be easy, comfortable and efficient. Yet, for the sake of comfort and simplicity, much user power is lost. While many users enjoy the limited but easy functionality offered by online cloud applications, in doing so, they are conferring more power to the service providers who actually control the communication infrastructure. The open protocols of the decentralized Internet are shunted aside in the push to enhance user mobility. These devices are "tethered" to their central core, the types of functions that the devices can perform and the applications that they run are either pre-set or controlled by the "mother" system, often remotely.3

Moreover, given that the cloud is - by definition - predicated on a service-oriented architecture (Yoo, 2011) most user interactions with the cloud revolve around the purchasing of online services. That is, rather than obtaining copies to be stored on a local hard drive, either by purchasing copies or by downloading them, users simply purchase ephemeral services on a current needs basis - through a pay-per-view or pay-as-you-go model. Under this model, users are turned into passive service-consumers and information-takers, as opposed to being pro-active information-creators or information-sharers (Lametti, 2012). Indeed, as users with less computational capacity can only interact with the cloud in the manner envisaged by the service-provider, they passively consume content and other services as opposed to generating content themselves. Access to services becomes the norm, and streaming takes over as the dominant descriptor of user behaviour (Lametti, 2012). Obviously, increased reliance on online services puts users at great risk to the extent that they might eventually lose access to these services.

Finally, most of these devices interact within proprietary systems (walled gardens), so that users are often required to opt for one particular system while purchasing a device. The vertical integration model of the cloud is based on providing a wide variety of convenient and easy integrated services. This is intended to entice users to a system and to subsequently keep them on that system (user lock-in). The situation is further exacerbated by the lack of interoperability among the competing clouds systems available to the public (Dillon & al., 2010). While they appear comfortable and convenient for most users, once they buy in, users become bound – in the long term in most cases – to a specific, requisite technology or platform (Chow & al., 2009). Technological incompatibilities constitute indeed an effective and dominant business model for the creation of "walled garden" - closed non-interoperable systems whose content can only be accessed according to the terms and conditions established by the online operator, by means of either contracts or technology (Boone, 2008). Besides, due to the lack of interoperability between systems, once they have been exported into the cloud, personal information and user-generated content will be difficult to transfer from one system to another - thereby allowing for the service provider to dictate terms of engagement in a manner that was heretofore impossible on an open internet.

To conclude, in order to communicate on the Internet, users increasingly rely on technological platforms provided by third parties to access services which are themselves defined and provided by third parties. The result is that, today, most of the means of production (in terms of hardware resources, software, content or data) are concentrated in the hands of fewer, large internet service providers. Just as in the early days of network computing, whose systems often revolved around a powerful central "mainframe" and local "dumb terminals", it is perhaps ironic that, today - in spite of the new opportunities provided by recent technological advances - we may be moving towards an analogous model of centralized computing, albeit on a global scale.

[3] See e.g. the issue of remote content removal from Amazon who removed certain Kindle titles from sale - such as Animal Farm and Nineteen Eighty-Four by George Orwell - and remotely deleted these titles from purchasers' devices after discovering that the publisher lacked the rights to publish them.

B. From “user comfort” to “user obsequity”

With the advent of cloud computing, more and more hardware, software, and informational resources are exported into the "cloud" - where they are often controlled by large corporations mainly interested in the maximization of profits (Zhang & al., 2010). Data is no longer stored on individual users’ devices, but rather in large data centers consisting of thousands of servers linked together into one large virtual machine. Applications are no longer run by end-users on their own devices, but are merely made available to the public through a web-interface, to which users can connect at any time and from anywhere (Miller, 2008). With more reliance on cloud computing and centralized architectures, user devices become less powerful, less generative, and less capable of interacting with anything but the central server to which it is tethered (Giurgiu & al., 2009). Thus, while ubiquitous computing definitely provides users with a greater degree of quality and comfort (Erdogmus, 2009), it is also likely to hinder users’ autonomy and jeopardize their freedoms -- a situation that could be described as the “tyranny of comfort”.

In spite of the growing choice of services that are nowadays available to the public, and despite the new opportunities provided by ubiquitous mobile applications, control over these applications remains ultimately centralized (Jaeger & al., 2009). Thus, to the extent that the underlying technology of online applications determines the way people communicate with each other, users' freedoms may potentially be limited by the constraints imposed (either voluntarily or not) at the level of the user interface (Voas & Zhang, 2009). This is further aggravated by the fact that we are witnessing today a progressive rise of private ordering through the use of contractual arrangements and technological means, acting either as a complement or a supplement to the law (De Filippi & Belli, 2012). The problem is that there is, at the moment, no guarantee that regulation by the private sector remains compatible with the fundamental rights of users - especially with regard to the rights of privacy and freedom of expression (Kushida & al., 2011). Hence, perhaps ironically, the comfort and new opportunities of ubiquitous online services are likely to impinge upon the freedom of users (De Filippi & McCarthy, 2010) and ultimately reduce their autonomy (Lametti, 2012).

Most critical in this regard is the strong level of centralization that characterizes many cloud computing platforms - allowing cloud operators to control users’ communications and possibly censor them (Karhula, 2010), with obvious negative repercussions on user’s rights. Today, many operators already filter or block certain types of contents they do not consider suitable to their platforms (such as offensive or pornographic content, for example).4 Yet, cloud operators may also arbitrarily decide to censor online communications that could prejudice they own private interests (commercial or not) without taking into account the implications on users’ freedom of expression and freedom to access information (Lessig, 1997). This is especially true in the case of countries with repressive governments or censorship regimes (Harwit & Clark, 2001; Kshetri, 2010).

On a different (but related) note, centralized control over the means of communication can significantly distort the type of content that users are exposed to. Driven by economic interests, many cloud operators are indeed more likely to promote the dissemination of popular content which attracts a greater number of users and thus generates higher advertising revenues (Redden & Witschge, 2010), at the detriment of less popular, but not necessarily less important content which receives less visibility.

Thus, in the realm of cloud computing, user ubiquity and connectivity ultimately lead to user obsequity. And such obsequity relates to content as well. As resources move away from users to increasingly

[4] See e.g. the case of Facebook, which has been accused several times of political and religious censorship for suspending the accounts of hundreds of users accused of a “terms of service” violation for posting political statements or religious views. In addition, Facebook’s Terms of Service prohibits ‘obscene’ and ‘sexually explicit’ material – where the assessment of such material is unilaterally carried out by Facebook’s staff itself without passing through a judicial review. For more details, see De Filippi & Belli (2012).

centralized architectures with large processing power and virtually unlimited storage capacity, users gradually lose control not only over the means of communication, but also over the content of communication (Chow & al., 2009). Data stored in the cloud can be exploited by third parties without having to request authorisation from users, nor even to inform them of the matter (Jaeger & al., 2008). Besides, exporting data into the cloud is likely to prevent right holders from exercising their rights. If "code is law" (Lessig, 2006), the user interface represents a series of technological rules that precisely determine the manner in which users can access or use their data (Kaczmarczyk, 2010). This means that, in practice, cloud operators (as data holders) have more control over the data than the actual rights holders (Wallis & al., 2011): on the one hand, they can ignore the license of works licensed under liberal licences - such as Creative Commons - given that these works are merely made available to the public over an online interface (Mowbray, 2009); on the other hand, cloud operators can implement (either voluntarily or not) the user interface with additional restrictions that extend beyond the standard level of protection granted by the copyright regime (Jiang, 2010) - potentially even constraining the access and reuse of works that are in the public domain (De Filippi & Vieira, 2013).

Privacy, confidentiality and data protection laws have also been severely impaired by the advent of cloud computing (Takabi & al., 2010), as much of the information that end-users would have normally stored on their computers is increasingly exported into foreign data centers (Dikaiakos & al., 2009) whose whereabouts cannot easily be established in advance (Svantesson & Clarke, 2010). Since cloud operators can monitor most of the communications and activities taking place on their platform (Lanois, 2010), they can potentially collect a variety of personal data, provided either intentionally or unintentionally by users. This information can subsequently be exploited, either directly by the cloud operators, or indirectly by selling it to third parties (Davis & Sedsman, 2010). Hence, while many cloud services are provided to users apparently for free, users actually pay for these services with their own data (Robinson, 2010). Yet, given that no money is being transferred, such transaction is often invisible to users, who have no opportunity to negotiate the terms of the agreement (Pater & al., 2009). Oftentimes, the privacy policies of cloud operators are neither read nor properly understood by end-users (Bezzi & Trabelsi,2011), and many stipulate that the terms and conditions may actually change over time without further notice (Bradshaw & al., 2011). Finally, although users are often willing to disclose personal information in exchange of a more personalized service (Guo & al., 2009), such information is often aggregated into large databases in order to extract or infer additional information (Bollier & Firestone, 2010), whose processing has never been explicitly authorized by users.

While users could theoretically chose to avoid services that impinge upon their fundamental rights, the higher is the level of centralization, the smaller is the number of alternatives that users can choose from (Haraszti, 2010). Moreover, although users could theoretically bring proceedings against online operators violating their rights, most cloud services are delivered by a multitude of actors (subcontractors) whose identity is generally unknown to end-users (Mowbray, 2009). This makes it difficult to determine in advance what would the applicable law be in case proceedings were brought (Ward & Sipior, 2010).5 Moreover, many of these operators do not have a direct contractual relationship with users, so that users can not seek recourse against them without passing through a long chain of intermediaries connected through a complex chain of contractual relationships.

[5] As Gellman (2012) points out, "[t]he user may be unaware of the existence of a second-degree provider or the actual location of the user's data [and] it may be impossible for a casual user to know in advance or with certainty which jurisdiction's law actually applies to information entrusted to a cloud provider."

Solutions and recommendations

A. User-driven grass-root solutions

After an initial period of euphoria on the part of users who enjoy the benefits of ubiquitous access to a growing number of online services, the dangers of ubiquitous computing and mobile applications are becoming more apparent. indeed, most of these benefits come along with variety of threats, security concerns (Stajano & Anderson, 2002), privacy and consumers risks (Svantesson & Clarke, 2010), as well as several social, economic and ethical implications (Bohn & al., 2005). Users have become increasingly aware that more and more online applications are governed by centralized entities controlled by private companies and governments, with the ability to monitor, manage and control network communications (Andrejevic, 2007).

While many users willingly submit to this incremental loss of autonomy, the most savvy of them are developing alternative platforms based on decentralized architectures. Unlike the majority of cloud services relying on the use of dumb terminals specifically designed to control and monitor user activities and communications, decentralized platforms are meant to encourage users to reacquire ownership and control over the resources that had been previously exported onto the cloud (Mosch, 2011).

Theses platforms generally rely on peer-to-peer technologies, allowing for computing resources (such as memory, storage, or processing power) to be shared by direct exchange amongst the peers in the network, without requiring the intermediation of any centralized server or associated authority (Androutsellis-Theotokis & Spinellis, 2004). At first, considerable attention was put on developing peer-to-peer applications for improving content distribution on the Internet. This is illustrated by the growing number of file-sharing networks that emerged over the past few years - such as Gnutella, eDonkey and BitTorrent, to name a few - which are nowadays considered to induce the largest amount of network traffic on the Internet. Popular peer-to-peer applications also includes online streaming (such as P2PTV or DPTP for audiovisual works, Freecast for music), online file storage (such as Wuala or Buddy Backup), and collaborative tools for content production (such as Kune). Peer-to-peer technologies have been subsequently deployed in many other fields and activities, such as social media (e.g. Diaspora), distributed search engines (e.g. YaCy, Faroo). anonymous browsing and internet communication designed to bypass censorship and control (e.g. FreeNET, i2p, TOR), or even digital currency (e.g. BitCoin).

More recently, Eben Moglen's extensive research concerning the dangers of ubiquitous online applications in the context of cloud computing (Moglen, 2011) has led to the development of the "Freedom Box" - a device designed to facilitate the creation of a decentralized architecture enabling users to exchange information and communicate securely, away from any corporate or governmental control. Technically, the Freedom Box consists of a small plug server that relies on free software and peer-to-peer technologies to establish a decentralized network of peers (where every peer contributes with a small amount of resources to the network) allowing users to communicate more freely and autonomously on the Internet.6

Decentralisation has recently gone one step further, moving from the mere application or logical layer to the actual infrastructure of the network through the development of wireless ad-hoc networks ("mesh networks") connecting users to one another in a peer-to-peer fashion. By using user devices (such as mobile phones, WiFi routers, etc) simultaneously as an access point and a relay node for other users (Akyildiz & al., 2005; Hassna & al., 2006) mesh networking allow people to communicate within a local community without having to pass through any centralized ISP (Dibbell, 2012).

Decentralized peer-to-peer architectures provide a series of benefits that might eventually restore the autonomy of Internet users. In terms of ubiquity and connectivity, they are such as to improve scalability

[6] More info available at http://freedomboxfoundation.org/

and network performance by accommodating transient populations of users (Androutsellis-Theotokis & Spinellis, 2004); they can increase the resiliency of the network by avoiding dependency on centralized servers ("single points of failure"); they help preserving proper connectivity while eliminating the need for costly infrastructure by aggregating resources and providing direct communication among peers (Milojici & al., 2002).

Moreover, by means of peer-to-peer technologies, these platforms can reestablish the original architecture of the Internet, designed as a decentralized system characterized by a network of peers interacting together with no hierarchical structure nor imbalance of power. Although it is sometimes possible to identify one or more entities in charge of administering or coordinating these networks, the regulation thereof is generally based on a decentralized system of governance. Thus, as opposed to the top-down approach to regulation adopted by many cloud operators, decentralized alternatives rely on bottom-up regulation, whereby the members of the community establish themselves the rules to which they want to abide (De Filippi & Belli, 2012).

Finally, the decentralized architecture of peer-to-peer networks is likely to provide users with a means to preserve anonymous communications, while resisting online surveillance and censorship. Anonymity is guaranteed as anyone can join and leave the network at any moment without having to ascertain their identity - although identification might nonetheless be required for accessing private or personal files (Ozhahata & al., 2005). Besides, given that packets travel from one peer to another in a decentralized fashion, there is no central authority responsible for routing communications throughout the network. This, in conjunction with sophisticated cryptographic techniques, makes it impossible for anyone to autonomously monitor, filter and/or censor online communications without involving the overall network of peers (Endsuleit & Mie, 2006).

However, in spite of their benefits, decentralized systems are often difficult to use and not as comfortable as many cloud-based services. They nonetheless play an important role insofar as they can protect users against potential abuses by online intermediaries. Indeed, to the extent that these networks operate autonomously and independently from the infrastructure of large operators, users do not have to abide to the terms and conditions imposed by cloud providers. As such, they represent a potential alternative to the commercial offers of dominant cloud providers (De Filippi & Belli, 2012).

Users often chose to surrender some degree of privacy or autonomy in exchange of a service whose benefits are perceived to be worth the costs. Yet, the harsher the terms of use and the weaker the respect for privacy and user rights are, the less willing users will be to trade-off freedom and autonomy for more comfort and accessibility (Dinev & Hart, 2003). The deployment of decentralized networks can therefore be regarded as an effective counter-power capable of indirectly regulating the operations of large cloud service providers, by preserving the ability for users to shift towards more decentralized alternatives, in the eventually that these services would become too "foggy" or "nefarious".

While these networks needs to reach a critical mass of users in order to be viable and function properly, they do not have to be as big, nor as good as most of the cloud services they compete with. As long as such networks exist, Internet users will enjoy the possibility of becoming more independent from large cloud operators. Their mere existence constitutes therefore a safeguard for users eager to regain greater autonomy and freedom of communication, or who are no longer satisfied with the growing encroachments on privacy and civil liberties implemented by cloud operators.

And certainly there will always be a role for persons versed in the technology -- the so-called hackers and geeks. As the pioneers of the digital realm, they test limits, probe technologies, identify the dangers, the vulnerabilities, the unethical or inappropriate business behaviors of cloud operators - ultimately serving as technological "watchdogs" in the cyberspace (Thomas, 2003).

B. Government intervention and collective user-oriented solutions

In addition to the user-driven responses described above, governmental intervention, combined with collective user-oriented solutions could be devised in order to address the twin challenges of ubiquity and autonomy in the cyberspace. The nature and viability of these solutions depend, to a large extent, on the social and political context in which they operate - which will ultimately determine the success or failure of various typologies of collective action. In particular, governmental intervention and formal government-driven solutions will be successful only where such intervention is seen as legitimate and to some extent desirable by the public. Community-based solutions, either formal or informal, will best succeed when driven by strongly committed actors whose actions are regarded as both credible and legitimate. In societies where the private sector is predominant and individual rights such as freedom of contract are cherished, instead, both formal and informal collective action might be better achieved by civil society organisations that operate beneath governmental administrations.

Regardless of the typology of actors behind these initiatives, different mechanisms might be employed as an attempt to resolve the growing challenges of cloud computing (as regards user privacy and autonomy) by focusing either on regulation or on the provision of alternative online platforms designed to better comply with users' rights and freedoms.

As for the former approach, it is our view that both government and inter-government solutions are needed. With regard to privacy, in particular, in spite of the international scope of cloud computing, domestic data protection laws could act as a baseline of protection to counterbalance the lack of bargaining power on the part of users and preserve the nature of privacy as a fundamental right (Rubenfeld, 1989). While users may by agreement or action either formally or effectively waive such protections,7 the baseline should be set such that the cloud architecture is constructed and maintained with privacy at the forefront. Yet, governments need to cooperate in order to apply these principles around the world. Indeed, divergences amongst national regimes - most notably between strong data protection regulations in Europe and weaker privacy laws in the U.S., where most cloud computing operators are based - could de facto annihilate the legal protection granted to the citizens of one country insofar as the data is exported into a foreign data center (De Filippi & Porcedda, 2012).

States could also assume - either directly or indirectly - an educational function so as to make users more aware of their rights in the Internet context. Only in this manner will users be able to protect and enforce their rights whenever they choose to, taking steps to put dubious practices under scrutiny and bring violators to justice. In addition, and perhaps equally important in practice, increased awareness will allow users to waive their rights in a more informed fashion - whenever they actually can and choose to do so.

As regards users' autonomy and freedoms, a number of formal government solutions might be advanced to help protect users. Using regulatory norms and instruments, governments might attempt to create

---

[7] In certain countries, privacy is a fundamental right which cannot be contracted around nor waived freely. In Europe, for instance, any agreement by an individual to waive some or all of the rights granted under the Data Protection Directive is both void and unenforceable - even if such agreement would actually further the interests of the data subject (Bergcamp, 2002). Yet, EC case-law and doctrine suggest that the "ban on waiver of data protection rights means not a ban of voluntary exchange of personal information for money, goods, or services, but prohibition of giving away for remuneration of, among others, the right to consent. Therefore, commercial exchange of personal data is not, in principle, outlawed" (Purtova, 2010). For more details on the case-law of the European Court of Human Rights as regards the waiver of rights, see De Schutter (2000) referring to e.g. *Bulut v. Austria*, Application No. 17358/90, Judgement of 22 February 1996, para. 30; *Deewer v. Belgium*, Judgement of 27 February 1980 published in Ser. A, Vol. 35, p. 56.

7

7

normative standards to regulate publicly-available cloud and internet services provided by the private sector. Thus, consumer protection standards might be used to regulate contracts in this context, especially contracts of adhesion, in which users purchase internet services but have little bargaining equality (Kessler, 1943). The rights of freedom of expression and freedom to obtain information can be relied upon in order to preclude online intermediaries from arbitrarily filtering or censoring online communications without any legitimate grounds (Cohen-Almagor, 2012). Competition and antitrust laws might also be used to ensure that major service providers compete in an open and meaningful manner, discouraging practices that would tend to greatly diminish either the number of providers or the variety of services offered to users (Sluijs, 2010). For instance, governments could mandate minimum standards of interoperability and portability, preventing large cloud operators from locking users into any one service. This might be implemented, in Europe, through an obligation for online operators to allow users to switch across services by transferring content from one to another with no technical or legal impediment.8

Alternatively, or as a complement to regulation, governments, public institutions (such as quangos, public research institutions or universities) and community organizations might respond by providing their own cloud-based solutions and providing their services to certain communities, segments of the population or indeed the population at large. Such responses would enable users to interact on the cloud, taking advantage of its ubiquity, without giving up their privacy or autonomy. As is the case for user-driven alternatives, collective solutions need not be as comprehensive as the cloud solutions offered by the private sector; they merely have to be a viable alternative that stands in effect as an insurance policy against the concentration of cloud power in the hands of a few.

From a governmental perspective, this can be done either indirectly, by setting up industry standards as regards accessibility, costs, interoperability and privacy rules (such as to positively direct the operations of the private sector), or directly, by providing such services themselves. The latter option can be achieved either through the creation of specific government agency or quango, or in the form of public-private partnership. For example, a government (or a group of governments acting in concert) might wish to provide cloud computing services to the general public at no or low cost, in order to ensure that all citizen-users have access and can benefit from the cloud computing potential. The implementation choice will depend on the administrative governance models particular to any given country or group of countries, and on the computing capacity at the government's disposal. Thus, in countries with a broad system of public universities or quangos with excess computing capacity,9 governments may use this option to provide internet services to a wide segment of the community. They may do so either by subsidizing these actors for providing such services or by providing a series of more indirect incentives. Alternatively, in countries with an under-developed framework of computing, private universities or private computing entities might be able to work with government to provide services respecting privacy and autonomy standards determined by the domestic law. Indeed, several private entities providing public cloud services may be willing to enter into agreements with governments to re-allocate some of their excess capacities in order to provide public services on their own platforms.

Finally, beyond the government and the private sector, specific communities might intervene by providing community clouds services and commons-based initiatives - some of which have already become an integral part of the Internet landscape.10 By providing direct services to their communities, these initiatives are extremely responsive to user needs, and thereby provide a useful barometer for the

---

[8] See Article 18 of the proposal for the new Data Protection Regulation in Europe, which introduced provisions for data portability imposing that users are given the opportunity to retrieve their data in a 'structured and commonly used' electronic format.

[9] Excess computing capacity in private entities like Amazon and Apple is, in fact, what led to the development of cloud computing technologies in the first place.

[10] Most popular examples community-driven online services based on cloud computing include, *inter alia*: Wikipedia.org; OpenStreetMap.org, a collaborative project to create a free editable map of the world; Sourceforge.net, a web-based source code repository for open source software development.

kinds of services users most need. As they might with public or private entities, governments might thus partner also with community groups by providing specific resources (such as facilities or hardware infrastructures), financial grants or subventions, and so forth.
To conclude, it bears repeating that the extent of governmental or community-driven initiatives in providing ubiquitous online services need not be as extensive as those services provided to the general public by the private sector. They need only be extensive enough to provide a meaningful alternative, so as to encourage private actors to adopt equivalent or better standards.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This chapter has provided an overview of the various advantages and drawbacks of ubiquitous computing, with particular focus on the most recent developments in cloud computing and the impact these developments might have on the exercise of fundamental users rights and freedoms. Attention has been drawn to the growing trend towards centralization that characterizes many online platforms, and the dangers that such centralized platforms present as regards the inherent loss of user autonomy and the potential violation of privacy rights and freedom of expression.

The objective of the chapter was not merely to describe the current state of affairs, but also - and mainly - to provide a prospective analysis of emerging trends in the context of cloud computing so as to identify the major challenges that will have to be addressed in the coming years. Most of the concerns identified above are, at the moment, still at an early stage of development. While they might eventually come true, as users seem to become more and more willing to trade-off their rights in the name of comfort and accessibility, this trend can nonetheless be reversed - or to the least obstructed - by properly informing users of what their rights are and how they could effectively be limited by large online operators abusing their dominant position in the market for cloud services.

Thus far, limited research has been done to understand the relationship between ubiquitous computing and user autonomy.11 While the present analysis present valuable insights with a view to generate awareness on this emerging issue, more research is needed to determine the extent to which our fears are actually coming true. Most critical in this regard is the need to monitor and to understand how cloud providers' policies and terms of use can actually affect user's preferences and behaviors in ubiquitous online platforms such as cloud computing. For instance, it is worth noting that increasingly intrusive privacy policies ultimately had divergent effects on user's behaviors: while many users simply submitted to the idea that "online privacy is dead" (Rauhofer, 2008), others actually decided to react by implementing alternatives solutions based on decentralized technologies that could eventually compete with the services currently offered by major cloud operators. In this last regard, more research should be undertaken in assessing the role of user- and community-driven initiatives acting as a counter-power to established commercial offers, as well as to investigate the effectivity of governmental regulation and public initiatives in counteracting the emerging trends in cloud computing.

[11] See, in this regards, Barkhuus & Dey (2003), Zittrain (2003, 2006, 2009), Bohn & al. (2005), Brey (2005), Greenfield (2006), Spiekermann & Pallas (2006), Hardian & al. (2006), Moglen (2010, 2011), De Filippi & McCarthy (2011, 2012), Lametti (2012).

REFERENCES

Andrejevic, M. (2007). Surveillance in the digital enclosure. *The Communication Review*, *10*(4), 295-317.

Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys (CSUR)*, *36*(4), 335-371.

Akyildiz I.F., Wang X., Wang W. (2005). "Wireless Mesh Networks: A Survey" in Computer Networks – Elsevier Science no. 47, Jan.

Banerjee, P., Friedrich, R., Bash, C., Goldsack, P., Huberman, B. A., Manley, J., ... & Veitch, A. (2011). Everything as a service: Powering the new information economy. *Computer*, *44*(3), 36-43.

Barkhuus, L., & Dey, A. (2003). Is context-aware computing taking control away from the user? Three levels of interactivity examined. In *UbiComp 2003: Ubiquitous Computing* (pp. 149-156). Springer Berlin/Heidelberg.

Bell, G., & Dourish, P. (2007). Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. *Personal and Ubiquitous Computing*, *11*(2), 133-143.

Bergkamp, L. (2002). EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy. *Computer Law & Security Review*, *18*(1), 31-47.

Bezzi, M., & Trabelsi, S. (2011). Data usage control in the future internet cloud.*The future internet*, 223-231.

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., & Rohs, M. (2005). Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. *Ambient intelligence*, 5-29.

Bollier, D., & Firestone, C. M. (2010). *The promise and peril of big data*. Aspen Institute, Communications and Society Program.

Boone, M. S. (2008). Past, Present, and Future of Computing and Its Impact on Digital Rights Management, The. *Mich. St. L. Rev.*, 413.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. *International Journal of Law and Information Technology*, *19*(3), 187-223.

Brey, P. (2005). Freedom and privacy in ambient intelligence. *Ethics and Information Technology*, *7*(3), 157-166.

Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on* (pp. 5-13). IEEE.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009, November). Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (pp. 85-90). ACM.

Cohen-Almagor, R. (2012). Internet Architecture, Freedom of Expression and Social Responsibility: Critical Realism and Proposals for a Better Future.

Davis, M., & Sedsman, A. (2010). Grey Areas-The Legal Dimensions of Cloud Computing. *International Journal of Digital Crime and Forensics (IJDCF)*, *2*(1), 30-39.

De Filippi, P., & Belli, L. (2012). The Law of the Cloud v the Law of the Land: Challenges and Opportunities for Innovation. *European Journal of Law and Technology*, *3*(2).

De Filippi, P., & McCarthy, S. (2011). Cloud Computing: Legal Issues in Centralized Architectures. In *VII International Conference on Internet, Law and Politics*.

De Filippi, P., & McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. *European Journal of Law and Technology*, *3*(2).

De Filippi P., & Porcedda, M.G. (2012), Privacy Belts on the Innovation Highway, in Proceedings of Internet, Politics, Policy 2012: Big Data, Big Challenges?, Oxford Internet Institute, University of Oxford, 20-21 September 2012.

De Filippi, P., & Vieira, M. (2013), The commodification of Information Commons. *International Journal of the Commons, Special Issue : The Knowledge Commons : from historical open science to digitally integrated research networks*, June 2013 (forthcoming).
De Schutter O. (2000). Waiver of Rights and State Paternalism under the European Convention on Human Rights. N. Ir. Legal Q. 51: 487.
Dibbell, J. (2012). The Shadow Web. *Scientific American*, *306*(3), 60-65.
Dikaiakos, M. D., Katsaros, D., Mehra, P., Pallis, G., & Vakali, A. (2009). Cloud computing: Distributed Internet computing for IT and scientific research.*Internet Computing, IEEE*, *13*(5), 10-13.
Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: Issues and challenges. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on* (pp. 27-33). IEEE.
Dinev, T., & Hart, P. (2003). Privacy concerns and Internet use–a model of trade-off factors. In *Best Paper Proceedings of Annual Academy of Management Meeting, Seattle*.
Endsuleit, R., & Mie, T. (2006, April). Censorship-resistant and anonymous P2P filesharing. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on* (pp. 7-pp). IEEE.
Erdogmus, H. (2009). Cloud computing: Does nirvana hide behind the nebula?.*Software, IEEE*, *26*(2), 4-6.
Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2008, November). Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE'08* (pp. 1-10). Ieee.
Gellman, R. (2012, August). Privacy in the clouds: risks to privacy and confidentiality from cloud computing. In *Proceedings of the World privacy forum,*.
Giurgiu, I., Riva, O., Juric, D., Krivulev, I., & Alonso, G. (2009). Calling the cloud: Enabling mobile phones as interfaces to cloud applications. *Middleware 2009*, 83-102.
Greenfield, A. (2006). *Everyware: The dawning age of ubiquitous computing*. Peachpit Press.
Guo, H., Chen, J., Wu, W., & Wang, W. (2009, November). Personalization as a service: the architecture and a case study. In *Proceedings of the first international workshop on Cloud data management* (pp. 1-8). ACM.
Haraszti, M. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. R. J. Deibert, J. G. Palfrey, R. Rohozinski, & J. Zittrain (Eds.). MIT Press.
Hardian, B., Indulska, J., & Henricksen, K. (2006, March). Balancing autonomy and user control in context-aware systems-a survey. In *Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on* (pp. 6-pp). IEEE.
Harwit, E., & Clark, D. (2001). Shaping the internet in China. Evolution of political control over network infrastructure and content. *Asian Survey*, *41*(3), 377-408.
Hassnaa M.et al. (2006). "A Panorama on Wireless Mesh Networks: Architectures, Applications and Technical Challenges".
Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud?. *Journal of Information Technology & Politics*, *5*(3), 269-283.
Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. (2009). Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday*, *14*(5), 1-12.
Jiang, G. (2010). Rain or Shine: Fair and Other Non-Infringing Uses in the Context of Cloud Computing. *J. Legis.*, *36*, 395.
Junglas, I., & Watson, R. (2003). U-commerce: a conceptual extension of e-commerce and m-commerce.
Kaczmarczyk, K. (2010). Predicting the future of the anti-circumvention laws in the cloud-computing world.
Karhula, P. (2012). Internet censorship takes new forms. *Signum*, (3).
Kessler, F. (1943). Contracts of Adhesion--Some Thoughts About Freedom of Contract. *Colum. L. Rev.*, *43*, 629.
Kshetri, N. (2010). Cloud computing in developing economies. *Computer*,*43*(10), 47-55.
Kushida, K. E., Murray, J., & Zysman, J. (2011). Diffusing the cloud: Cloud computing and implications for public policy. *Journal of Industry, Competition and Trade*, *11*(3), 209-237.

Lametti, D. (2012). The Cloud: Boundless Digital Potential or Enclosure 3.0?.
Lanois, P. (2010). Caught in the clouds: The Web 2.0, cloud computing, and privacy. *Nw. J. Tech. & Intell. Prop.*, *9*, 29.
Leimeister, S., Böhm, M., Riedl, C., & Krcmar, H. (2010). The Business Perspective of Cloud Computing: Actors, Roles and Value Networks.
Lessig, L. (1997). Tyranny in the infrastructure. *Wired, July*.
Lessig L. (2006), *Code: And Other Laws of Cyberspace*, Version 2.0. Basic Books, NY.
Lyytinen, K., & Yoo, Y. (2002). Ubiquitous computing. *Communications of the ACM*, *45*(12), 63.
Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST special publication*, *800*, 145.
Miller, M. (2008). *Cloud computing: Web-based applications that change the way you work and collaborate online*. Que publishing.
Milojicic, D. S., Kalogeraki, V., Lukose, R., Nagaraja, K., Pruyne, J., Richard, B., ... & Xu, Z. (2002). Peer-to-peer computing.
Moglen, E. (2011). *Why Political Liberty Depends on Software Freedom More Than Ever*, 2011 FOSDEM conference, Brussels. February 5, 2011
Mosch, M. User-controlled data sovereignty in the Cloud. In *Proceedings of the PhD Symposium at the 9th IEEE European Conference on Web Services (ECOWS 2011), Lugano, Switzerland (September 2011)*.
Mowbray, M. (2009). The fog over the grimpen mire: Cloud computing and the law. *Scripted Journal of Law, Technology and Society*, *6*(1).
Ohzahata, S., Hagiwara, Y., Terada, M., & Kawashima, K. (2005). A traffic identification method and evaluations for a pure P2P application. *Passive and Active Network Measurement*, 55-68.
Patel, P., Ranabahu, A., & Sheth, A. (2009, October). Service Level Agreement in cloud computing. In *Cloud Workshops at OOPSLA*.
Plummer, D. C., Bittman, T. J., Austin, T., Cearley, D. W., & Smith, D. M. (2008). Cloud computing: Defining and describing an emerging phenomenon.*Gartner, June*, *17*.
Purtova, N. (2010). Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights. *Netherlands Quarterly of Human Rights*, *28*(2), 179-198.
Rauhofer, J. (2008). Privacy is dead, get over it! 1 Information privacy and the dream of a risk-free society. *Information & Communications Technology Law*,*17*(3), 185-197.
Redden, J., & Witschge, T. (2010). A new news order? Online news content examined. *New Media, Old News: journalism and democracy in the digital age*.
Robison, W. (2010). Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act. *Georgetown Law Journal*, *98*(4).
Rubenfeld, J. (1989). The right of privacy. *Harvard Law Review*, 737-807.
Spiekermann, S., & Pallas, F. (2006). Technology paternalism–wider implications of ubiquitous computing. *Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science*, *4*(1), 6-18.
Stajano, F., & Anderson, R. (2002). The resurrecting duckling: security issues for ubiquitous computing. *Computer*, *35*(4), 22-26.
Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review*, *26*(4), 391-397.
Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *Security & Privacy, IEEE*, *8*(6), 24-31.
Thomas, D. (2003). *Hacker culture*. University of Minnesota Press.
Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review,* 39(1), 50-55.
Voas, J., & Zhang, J. (2009). Cloud Computing: new wine or just a new bottle?.*IT professional*, *11*(2), 15-17.

Wallis, M., Henskens, F., & Hannaford, M. (2011). Web 2.0 Data: Decoupling Ownership from Provision. *International Journal On Advances in Internet Technology*, *4*(1 and 2), 47-59.
Watson, R. T., Pitt, L. F., Berthon, P., & Zinkhan, G. M. (2002). U-commerce: expanding the universe of marketing. *Journal of the Academy of Marketing Science*, 30(4), 333-347.
Ward, B. T., & Sipior, J. C. (2010). The Internet jurisdiction risk of cloud computing. *Information Systems Management*, *27*(4), 334-339.
Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7-18.
Zittrain J. (2003), Internet Points of Control, in 44 B. C. L. Rev 653
Zittrain J. (2006), A history of online gatekeeping, 19 Harvard Journal of Law and Technology 253.
Zittrain, J. (2009). *The future of the internet--and how to stop it*. Yale University Press.

ADDITIONAL READING SECTION

Andrejevic M. (2007), Surveillance in the Digital Enclosure, The Communication Review, Vol. 10 Issue 4
Balkin, Jack M. (2008), Media Access: A Question of Design (May 1, 2008). George Washington Law Review, Vol. 76, No. 4, 2008
Bendrath R., Milton Mueller (2011),The end of the net as we know it? Deep packet inspection and internet governance, New Media & Society November 2011 - vol. 13 no. 7 1142-1160
Benkler, Y. (2006) THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM.
Benkler, Y (1997), Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment.
Bettig R. (1997), The enclosure of cyberspace, Critical Studies in Mass Communication, Volume 14, Issue 2, 1997;
Boyle, J. (2008) THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND.
Burri, Mira, Controlling New Media (without the Law) (November 19, 2011). HANDBOOK OF MEDIA LAW AND POLICY, Monroe Price & Stefaan Verhulst, eds., Routledge, 2012; NCCR Trade Regulation Working Paper No. 2011/71
Clark, David D. (2010), The End-to-End Argument and Application Design: The Role of Trust, in 63 Fed. Comm. L.J. 357 (2010-2011)
Doctorow, C. (2012) Lockdown: The Coming War on General-Purpose Computing, BOING BOING (Jan. 13, 2012), http://boingboing.net/2012/01/10/lockdown.html.
Dyer-Witheford N. (2009), Cyber-Marx : cycles and circuits of struggle in high technology capitalism, Urbana : Univ. of Illinois Press, 1999;
Etro, Federico, The Economics of Cloud Computing (March 8, 2012). The IUP Journal of Managerial Economics, Vol. IX, No. 2, pp. 7-22, May 2011.
Frischmann, B. (2009) Spillovers Theory and Its Conceptual Boundaries, 51 WM. & MARY L. REV. 801..
Frischmann, B. (2012) INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES, Oxford UP.
Galuba W. (2008), Friend-to-Friend Computing: Building the Social Web at the Internet Edges, Working Paper, Ecole Polytechnique Fédérale de Lausanne (EPFL).
Gervais, D.J. & Hyndman, D. (2012) Cloud Control: Copyright, Global Memes and Privacy, 10 J. TELECOMM. & HIGH TECH. L. 53.
Granstrand, Ove (2000), The shift towards intellectual capitalism -- the role of infocom technologies, Research Policy, Vol. 9, Issue 29. Elsevier
Hintz, Arne; Milan, Stefania (2009), At the margins of Internet governance: grassroots tech groups and communication policy, in International Journal of Media & Cultural Politics, Volume 5, Numbers 1-2, 1 March 2009 , pp. 23-38(16)

Hood C., Helen Z. Margetts (2007),The Tools of Government in the Digital Age: Second Edition (Public Policy and Politics). Palgrave Macmillan, 2007
Karlekar K. and Sarah G. Cook (2008), Access and Control: A growing diversity of threats to internet freedom, in Freedom on the Web. Freedom House.
Klang M. (2006), Disruptive Technology: Effects of Technology Regulation on Democracy; Göteborg University.
Kushida K, Jonathan Murray, John Zysman (2011), Diffusing the Cloud: Cloud Computing and Implications for Public Policy, in Journal of Industry, Competition and Trade, Vol. 11, No. 3 pp. 209-237
Lametti, D. (2011), On Creativity, Copying and Intellectual Property in Roberto Caso, ed. Plagio e Creatività: Un Dialogo tra Diritto e altri Saperi (Trento; Università di Trento, 2011) pp. 171-89.
Lametti, D. (2011), The Virtuous P(eer): Reflections on the Ethics of File Sharing, in A. Lever, ed. New Frontiers in the Philosophy of Intellectual Property (Cambridge; CUP, 2011) pp. 284-306.
Lametti, D. (2010), The Objects of Virtue in G. Alexander and E. Peñalver, eds. Property and Community (New York; Oxford University Press, 2010) pp. 1-37.
Lametti, D. (2010), “How Virtue Ethics Might Help Erase C-32’s Conceptual Incoherence”, in M. Geist (ed), From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda (Toronto; Irwin Law, 2010) pp. 309-340.
Lametti, D. (2005), Coming to Terms with Copyright, in M. Geist (ed) In the Public Interest: The Future of Canadian Copyright Law (Toronto; Irwin Law, 2005) pp. 480-516.
Lemley, Mark A.; Lessig, Lawrence (2000), The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era, 48 UCLA L. Rev. 925 (2000-2001).
Lucas M. (2007), Decentralizing Digital Social Networking Applications. Working Paper, University of Illinois at Urbana-Champaign.
Madison M.J. (2003), Rights of Access and the Shape of the Internet, in 44 B.C. L. Rev 433
Mell, P. & Grance, T. (2011) NAT’L INST. OF STANDARDS & TECH., SPECIAL PUB. 800–145, THE NIST DEFINITION OF CLOUD COMPUTING 2–3.
Moglen (2010); Freedom in the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing.
Mukherji A. (2002) "The evolution of information systems: their impact on organizations and structures", Management Decision, Vol. 40 Iss: 5, pp.497 - 507
Murray A., Colin Scott (2002), Controlling the New Media: Hybrid Responses to New Forms of Power, The Modern Law Review, Volume 65, Issue 4, pages 491–516, July 2002
Oram A. (2001), Peer to Peer: Harnessing the Power of Disruptive Technologies.
Polanyi, K. (1944) THE GREAT TRANSFORMATION: THE POLITICAL AND ECONOMIC ORIGINS OF OUR TIME.
Reidenberg, Joel R. (1998), Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 Tex. L. Rev. 553 (1997-1998).
Sartor G. and Mario Viola de Azevedo Cunha (2010), The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents, Int J Law Info Tech (2010) 18 (4):356-378.
Sinnreicha A., Nathan Grahama & Aaron Trammella (2011), Weaving a New 'Net: A Mesh-Based Solution for Democratizing Networked Communications, The Information Society: An International Journal. Volume 27, Issue 5, 2011
Slujis, J. et al. (2011) TILBURG LAW & ECON. CTR., DISCUSSION PAPER 2011-036, CLOUD COMPUTING IN THE EU POLICY SPHERE.
Sørensen C., David Gibson, (2004) "Ubiquitous visions and opaque realities: professionals talking about mobile technologies", info, Vol. 6 Iss: 3, pp.188 - 196
Walker J. (2003), The Digital Imprimatur: How Big Brother and Big Media can put the Internet Genie back in the bottle, in Knowledge, Technology, and Policy, Fall 2003, Vol. 16 No.3, pp. 24-77

Weiser M. (1991). The computer for the 21st century. Scientific American, (Sept. 1991), 94–104.
Whitaker R. (2000), The End of Privacy. The New Press.
Willey D., Erin K. Edwards (2002) Online self-organising social system, in Michael Simonson, Charles Schlosser (eds.) Quarterly Review of Distance Education, Vol. 3. Number 1, 2002.
Ziccardi G. (2009), RESISTANCE, LIBERATION TECHNOLOGY AND HUMAN RIGHTS IN THE DIGITAL AGE, in Law, Governance and Technology Series, 2013, Volume 7, 27-71
Yoo, C.S. (2011), Cloud Computing: Architectural and Policy Implications, 36 REV. INDUS. ORGS. 405.

KEY TERMS AND DEFINITIONS

Cloud Computing: Defined by the NIST 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", cloud computing basically refers to any application or service running on a distributed network and relying on virtualized resources (i.e. resources that have been aggregated into a common pool to be subsequently shared amongst users) which can be easily accessed by common Internet protocols

Ubiquitous computing: Regarded as a common characteristic of many online applications, computing resources can be regarded as ubiquitous to the extent that they are time-, location- and device-independent, i.e. they can be accessed at any time, from anywhere, and regardless of the user device.

Peer-to-peer networks: We refer here to a peer-to-peer networks as any online infrastructure composed of multiple autonomous nodes that communicate through a network according to a specific protocol, without ever passing through a central node.

End-to-end principle: Considered by many as one of the fundamental design principles of the internet network, the end-to-end principle is also an important precondition for user autonomy. Indeed, the principle stipulates that the intelligence of the internet should subsist not in the network itself but rather at its end-points (i.e. at the level of users' devices). This means that the network should remain a mere (and neutral) means of communication, and that end-nodes are powerful enough to be running servers and providing online services for user interaction and online communication.

Tethered devices: "Tethered devices" are devices which the user cannot fully control, because the parent companies maintain a certain degree of control over these devices insofar as they can decide on their actual functionalities, the degree of interoperability with other devices, as well as the manner in which and the extent to which they can be used in any given situation. Mobile phones, mp3 players, consoles, tablets are common examples of tethered devices where the seller uses internet connectivity in order to control the use of the devices it sells to end-users.

Right to privacy and data protection: In the context of EU law, privacy and data protection are two intertwined fundamental rights enshrined in the European Charter of Fundamental Rights. The former protects individuals' private and family life (hence relations), private dwellings and communications via

any medium, while the latter safeguards the processing of data carrying information relating to identified or identifiable individuals (i.e. personal data).

Right to freedom of expression: The right to freedom of expression is recognized as a human right under Article 19 of the Universal Declaration of Human Rights and recognized in international human rights law in the International Covenant on Civil and Political Rights (ICCPR). Article 19 of the ICCPR states that "[e]veryone shall have the right to hold opinions without interference" and "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". Article 19 goes on to say that the exercise of these rights carries "special duties and responsibilities" and may "therefore be subject to certain restrictions" when necessary "[f]or respect of the rights or reputation of others" or "[f]or the protection of national security or of public order (order public), or of public health or morals"