Available online at www.sciencedirect.com
ScienceDirect
www.compseconline.com/publications/prodclaw.htm
Computer Law & Security Review

Property and the cloud

Cesare Bartolini [a,*], Cristiana Santos [b], Carsten Ullrich [c]

[a] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg
[b] Institute of Law and Technology, Autonomous University of Barcelona, Barcelona, Spain
[c] Faculté de Droit, d'Economie et de Finance, University of Luxembourg, Luxembourg, Luxembourg

Keywords:
Cloud computing
Property
Intellectual property
Copyright
Trade secret
Patents
Contractual terms
Dispute resolution
Data protection

ABSTRACT

Data is a modern form of wealth in the digital world, and massive amounts of data circulate in cloud environments. While this enormously facilitates the sharing of information, both for personal and professional purposes, it also introduces some critical problems concerning the ownership of the information. Data is an intangible good that is stored in large data warehouses, where the hardware architectures and software programs running the cloud services coexist with the data of many users. This context calls for a twofold protection: on one side, the cloud is made up of hardware and software that constitute the business assets of the service provider (property of the cloud); on the other side, there is a definite need to ensure that users retain control over their data (property in the cloud). The law grants protection to both sides under several perspectives, but the result is a complex mix of interwoven regimes, further complicated by the intrinsically international nature of cloud computing that clashes with the typical diversity of national laws. As the business model based on cloud computing grows, public bodies, and in particular the European Union, are striving to find solutions to properly regulate the future economy, either by introducing new laws, or by finding the best ways to apply existing principles.

1. Introduction

Cloud computing is a very important technological development which cloud-utilizing organizations (enterprise and government customers) and consumers are increasingly taking up on an as-needed basis. Within this property paradigm shift, enterprises outsource data processing capabilities, Internet-based resources, and delivery of IT applications, storage, and memory space to cloud services. Clients thus benefit from larger, scalable storage, processing capacities, and ubiquitous access to their data and preferred services, while the enterprise does not need to own such resources or perform their management and maintenance.

The cloud is also making the exploitation of Big Data possible[1], as it allows to move, share and reuse data seamlessly

* *Corresponding author.* Interdisciplinary Centre for Security, Reliability and Trust, Université du Luxembourg, 29, Avenue J.F. Kennedy, Luxembourg, L-1855, Luxembourg.
E-mail address: cesare.bartolini@uni.lu (C. Bartolini).

https://doi.org/10.1016/j.clsr.2017.10.005

[1] Alongside the data created by billions of people using digital devices and services for personal and professional reasons and data generated by the increasing number of connected objects, other sources of data are research, digitized literature and archives, and public services such as hospitals and land registries. Big Data creates new possibilities to share knowledge, to carry out research and to develop and implement public policies. It should be pointed out that "Big Data" is more of a buzzword used in industry and in research than a technical concept. There is no precise definition for Big Data, and its meaning can change according to the context. See Jacobs, "The Pathologies of Big Data."

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

across global markets and borders, and among institutions and research disciplines. The ability to analyze and exploit Big Data is having an impact on the global economy and society, opening up possibilities for major scientific, industrial and social innovations. A key part of this impact is the change in the way scientific research and knowledge are carried out, as the world is moving toward the open science paradigm and science clouds[2]. In this line, the *European Cloud Initiative*[3] builds on the *Digital Single Market* (DSM) Strategy, which aims, *inter alia*, at maximizing the growth potential of the European digital economy[4]. The plan is to develop a trusted, open environment, called the *European Open Science Cloud*[5], for the scientific community to store, share and reuse scientific data and results. The European Open Science Cloud would make science more efficient by better sharing resources at national and international levels[6].

While cloud services potentially bring about many tangible and varied benefits to end-users, they also come with numerous legal risks hampering its wide adoption. In addition to the economic implications that are beyond the scope of this work, several problems concerning cloud computing arise from a legal point of view. The traditional legal framework might be seriously jeopardized by the advent of cloud computing, especially concerning the concept of property. In particular, there exist two distinct perspectives under which property can be analyzed, and mixing them up can lead to confusion. On one side, there is the perspective of property *of* the cloud. Structurally, a cloud is a combination of hardware and software. The former consists of a set of material goods, subject to ordinary property rules, and circulating according to real estate laws. The software, on the other hand, is subject to the vast and complex framework of intellectual property rules, and generally governed by means of contracts and licenses. However, both must be regarded as business assets of the cloud provider, as neither the hardware nor the software is sufficient to run the cloud services without the other. As such, they are also encompassed by business law. The interaction of these three sets of rules stems some questions that this paper tries to address.

The opposite perspective concerns the property *in* the cloud. More often than not, cloud services collect and store data belonging to their users, or of the users of enterprises relying on those services in the case of a B2B paradigm[7]. This data, for example, can pertain to personal data (including pictures of the person), writings or other pieces of art (including photographs that cannot be regarded as personal data), school notes, technical documents used for work, private documents such as administrative material or accounting data, backup copies of purchased electronic materials such as books, music or movies, software under development, and so on. Clearly, cloud storage services[8] tend to have a larger variety of data that can be stored by end-users, but, in general, some amount of data is collected by any cloud service[9]. All this data raises very important questions concerning its property. Additionally, this data can be subject to protection according to its content (e.g., data protection, copyright, trade secrets, and the like), which further complicates its applicable legal regime.

Yet, no specific pan-European regulation has been elaborated so far embracing cloud computing. Although generally not strictly tailored for cloud computing, a large number of regulatory instruments apply to that domain[10], mostly concerning the non-material perspective of the cloud. These regulations generally focus on the contractual issues between the cloud service provider and other stakeholders, such as end-users or the businesses that rely on the cloud.

Consequently, the European Commission described the current context of cloud computing in harsh tones. It remarked a lack of legal certainty in terms of access and usage, restrictions to the free flow of data, a proliferation of unbalanced contracts with cloud providers who "use complex contracts or service level agreements with extensive disclaimers"[11], and the resulting risk of unfair contract terms being imposed on consumers. According to the Commission, this context has led to a lack of confidence in digital systems and a reluctance to use these services. Building a consumer-friendly legal and policy framework for cloud computing involves addressing a series of cross-cutting issues in multiple areas, such as data protection, copyright, consumer protection, trade secrets, licensing, security, dispute resolution and contract law, among other legal instruments, all while guaranteeing the neutrality of the Internet. The General Data Protection Regulation[12] and the forthcoming revision of EU copyright legislation[13] provide general frameworks that are relevant in this context. If an expectation of compliance is to be achieved

[2] Hoffa et al., "On the Use of Cloud Computing for Scientific Workflows." For the implementation of a cloud service for open science, see Grossman et al., "The Design of a Community Science Cloud."

[3] "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Cloud Initiative - Building a Competitive Data and Knowledge Economy in Europe."

[4] "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe."

[5] http://ec.europa.eu/research/openscience/index.cfm?pg=open-science-cloud (visited October 27, 2017).

[6] European Commission, *Results of the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy*.

[7] See *infra* at Section 2.

[8] Such as Dropbox.

[9] At the very least, the data required to securely access one's account.

[10] For an approach to assess the legal compliance of a cloud service, see Di Martino, Cretella, and Esposito, "Towards a Legislation-Aware Cloud Computing Framework."

[11] "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Cloud Initiative - Building a Competitive Data and Knowledge Economy in Europe."

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[13] "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Modern, More European Copyright Framework."

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

in this digital environment by any kind of information system, regulations, and their potential implications on cloud computing, must be made accessible to policy makers, business analysts and software developers, alike.

On one hand, cloud computing is not a uniform concept, but it represents a vast phenomenon that can operate under many different structures and configurations. On the other hand, there are many different legal regimes that can affect cloud computing, spanning different material and geographical scopes. This complexity lays the ground for a number of questions that can rise around cloud computing concerning the topic of property, and literature shows that many of them have been addressed to some extent. This paper aims at a more systematic analysis of the topic of property in cloud computing. The approach followed herein classifies property in cloud computing along two intersecting axes: one that separates the property of the components that provide the cloud functionality, which are essentially business assets, from that of the information stored in the cloud by its users; and another that examines the various legal regimes affecting cloud computing, producing different facets of property rights, each with its own consequences.

Due to the (normally) cross-border nature of cloud computing and the complexity of the legal landscape, it is hard to perform such an analysis sticking rigidly to specific jurisdictions. As a general rule, the pivot of the study will be European law, as its Digital Single Market strategy is building a comprehensive legislation of the digital world that is uniform across the Union. However, most cloud services used within European countries belong to enterprises based in the United States, where legislation tends to be significantly different. As the applicable law can significantly affect the business opportunities, for most of the legal regimes under study it will be necessary to provide at least a high-level overview of the legal tensions created between Europe and the U.S. Additionally, where European law may not be sufficient to describe a legal domain[14], a comparative analysis of the national law of some countries will be performed.

As the focus of this paper is on a property perspective, it does not cover other topics in cloud computing, such as legal compliance[15], breach of contract, and the economics of cloud computing, user trust[16], unfair contracts[17], or remedies. Although some of these topics are mentioned and superficially discussed in some sections of the present work, their detailed analysis offers a separate topic of investigation.

The structure of the paper is the following. Initially[18], a preliminary, brief description of cloud computing will be given, highlighting some of its most relevant classifications. Then the issues concerning the property of the cloud assets will be addressed[19], covering the main legal regimes that affect them, from the point of view of both material and intellectual property. The opposite perspective of the information stored in the cloud will be analyzed next[20], mainly in the light of intellectual property (as only immaterial goods can be stored in a cloud), liability, competition law, and data protection. The conclusions[21] will draw some final remarks and cast an eye in an evolutive direction.

2. From traditional software to the cloud

The emergence of modern technologies has caused a shift in the traditional computing paradigm. The concepts of service-oriented architectures and cloud environments, in particular, have significantly blurred the edges of the legal context in which computing occurs.

The traditional approach to software is pretty straightforward. Classical software is developed by individuals or enterprises, who consequently own the intellectual property rights. The software is protected by copyright law, and its distribution is by means of physical media (the *corpus mechanicum* of intellectual property) which users can purchase. In this model, software is no different from other intellectual properties: users own the physical media and not the software, but they are entitled to use it on the basis of software licenses. However, as the use of a software is bound to the material apprehension of the physical medium on which it resides, the opportunity to replicate the content of the (cheap) physical media makes it difficult to protect the intellectual property rights. Industry developed a wide variety of measures to restrict such replication[22], but none of them has proven particularly effective insofar as the protected content could circulate entirely on a physical medium.

The diffusion of the Internet and the emergence of new technologies, protocols and development models brought forth new paradigms for software development. The various forms of distributed computing, such as grids, service-oriented architectures, and ultimately cloud computing, have significantly changed the pre-existing scheme. A large amount of today's software is not distributed via physical means, but through services hosted by the software vendor. In its essence, this means that software users generally obtain a front-end, which is not sufficient *per se* to offer the functionality, but it relies on external resources. Users can access such resources over the Internet, generally by creating an account that is stored on the vendor's database[23]. As argued *infra*[24], this model offers a better

[14] As in the case of real estate law. See *infra* at Section 3.1.

[15] For the topic of legal compliance, see Helmbrecht, "Data Protection and Legal Compliance in Cloud Computing"; Casalicchio and Palmirani, "A Cloud Service Broker with Legal-Rule Compliance Checking and Quality Assurance Capabilities."

[16] The issue of user trust is being studied by the Commission; see for example *Cloud Security Workshop: Building Trust in Cloud Services - Certification and Beyond*.

[17] Expert Group on Cloud Computing Contracts, *Unfair Contract Terms in Cloud Computing Service Contracts Discussion Paper*.

[18] Section 2.

[19] Section 3.

[20] Section 4.

[21] Section 5.

[22] For an in-depth analysis of the topic, see Marks and Turnbull, "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses"; Kerr, Maurushat, and Tacit, "Technical Protection Measures: Tilting at Copyright's Windmill."

[23] Wang et al., "Cloud Computing: A Perspective Study" offer a high-level description of cloud computing and its main features, as well as a simplified overview of its difference from other paradigms such as grid computing.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

protection of intellectual property rights: as long as essential parts of the software are not distributed but only accessed via the front-end, the vendor can easily ensure that only licensed users have access to the software functionality.

A corresponding shift in the business model occurred. Specifically, while the business model where users have to pay for the software still exists, a large amount of software is available free of charge. While the traditional model provides revenues in a manner that is essentially similar to the sale of goods (as is entails the transfer of the property of the physical support along with the license to use the software), this second model is closer to a provisioning of services, and the revenues for the enterprise can come not as a price in a sale of material goods or as a licensing fee for intellectual property, but in other forms: typical examples are usage fees for the service[25], personal data to sell to third parties for advertising purposes[26], enhancements and extensions that are not available in the free software but can be purchased separately (often through in-app purchases), or customer support for the software[27].

2.1. *Cloud computing and its classifications*

Cloud computing[28] is a modern IT structure in which part of the software or hardware resources are not in the hands of the user, but they are located on some remote server and accessible through the Internet. The remote resources are called the *cloud*. According to the terms of service of contracts, and by means of interfaces and tools, users can access the cloud.

Cloud computing comes in different flavors, called delivery models, which differ by the amount and type of assets that are located on the cloud. Three delivery models are commonly used[29]:

- *Software as a Service* (SaaS) is the evolution of traditional service-based software, where the user accesses the software, or part of it, remotely. Generally, this delivery model is at the basis of a B2C business model, because the cloud provider offers services directly to end-users;
- *Platform as a Service* (PaaS) offers a set of assets to store software in the cloud, and a uniform set of facilities and services for their management and interoperability;
- *Infrastructure as a Service* (IaaS) has a wider scope, since it also offers computing power (in the form of virtual machines) and communication resources.

Fig. 1 displays a popular diagram summarizing the differences between the various delivery models. Other, less known, types of cloud exist, such as *Hardware as a Service* (HaaS) or *Data as a Service* (DaaS). In general, it is recognized that every portion of computing can be delivered as a service[30].

[24] Section 3.3.1.

[25] This is the usual business model for cloud services catering to enterprises. A paramount example is Amazon Web Services, which offers infrastructure, storage, and even computational power (in the form of virtual machines) on which a large number of other cloud providers rely. This kind of business model normally requires a fee based on the nature and amount of resources used by the customer (e.g., the size of the storage space), either statically (the customer pays a fixed amount for a limited number of resources and cannot use any more than those) or dynamically (the customer pays a fixed quota for the subscription, plus an additional amount depending on the resources that are actually used, which are allocated by the service on demand).

[26] The European Commission recognizes the value of personal data as an essential part of the business model. According to "European Commission - Fact Sheet: Questions and Answers - Data Protection Reform," "Data is the currency of today's digital economy. Collected, analysed and moved across the globe, personal data has acquired enormous economic significance. According to some estimates, the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020. By strengthening Europe's high standards of data protection, lawmakers are creating business opportunities".

[27] The Linux operating system distributions frequently make use of this model. Linux distributions (and other popular open software products) are often backed by a company that provides two types of product: the community version, supported by a large community of independent developers and enthusiasts but not offering any kind of professional assistance, and the enterprise version, which offers several degrees of professional assistance for technical support. See Rappa, "The Utility Business Model and the Future of Computing Services," where this form of business is defined "community model".

[28] It is not easy to provide a definition of cloud computing. The definition depends on the author but also on the context in which it is used. According to Armbrust et al., "A View of Cloud Computing," "[c]loud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services". An official definition is offered by Mell and Grance, "The NIST Definition of Cloud Computing": "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [. . .] with minimal management effort or service provider interaction". Five essential characteristics are declared within the document: (i) on-demand self-service (automatic provisioning of computing), (ii) broad network access (services available over a networked infrastructure), (iii) resource pooling (resources are pooled together to serve multiple consumers using a multi-tenant model), (iv) rapid elasticity (rapid and elastic provisioning of capabilities to quickly scale up or down as required) and (v) measured service (automatic control and optimization of resources utilizing a pay-per-use model).A rich survey of existing definitions of the cloud is presented by Vaquero et al., "A Break in the Clouds: Towards a Cloud Definition," concluding that a cloud is "a large pool of easily usable and accessible virtualized resources [. . .] typically exploited by a pay-per-use model [. . .]".The EU recognized the importance of the cloud technology in a strategic document (see "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe"), where it is defined as the storing, processing and use of data on remotely located computers accessed over the internet.

[29] It is not easy to track down the exact origin of these terms. The first reference to software as a service appears to be in Bennett et al., "Service-Based Software: The Future for Flexible Software.", although the acronym is first used in the whitepaper Software & Information Industry Association, *Software as a Service: Strategic Backgrounder*. In the context of cloud computing, an overview of the various delivery models can be found in Vaquero et al., "A Break in the Clouds: Towards a Cloud Definition"; Subashini and Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing."

[30] Schaffer, "X as a Service, Cloud Computing, and the Need for Good Judgment."

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

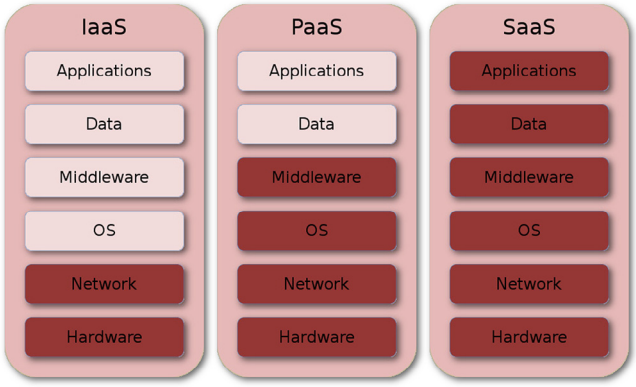

Fig. 1 – Difference between cloud types.

The delivery models differ in which parts of the computing process are located on the CSP. Of course, the complexity of the services offered and the interfaces to use them change accordingly. In addition to the technical structure, the organizational and legal aspects also depend strongly on the delivery model. A large delivery model, providing most of the technical assets required by its customers, requires a big organization and a high degree of efficiency. The liability for damages in a larger delivery model can be significantly higher in the more extensive delivery models such as IaaS[31].

Additionally, the three main delivery models (SaaS, PaaS and IaaS) often operate in a hierarchical structure. Providers of software services nowadays have to deal with the high fluctuation of demand: since the context is different from the past, when it was possible to estimate the peak hours and allocate server resources to serve to peak, in the age of ubiquitous computing the demand becomes much more unpredictable. Providers of SaaS services thus tend to rely on the outsourcing of assets on a PaaS cloud, which dynamically manages the resource allocation of resources to the hosted SaaS services[32]. On a larger scale, this structure can be replicated in the interaction between PaaS and IaaS architectures. The complexity of such a model is one of the reasons why there is a need to make the ownership of the respective assets clear.

Another classification of clouds concerns their architecture, which can be single-tenant or multi-tenant, although the multi-tenant model is becoming predominant due to the lower amount of resources it requires[33]. In the single-tenant model, multiple, separate instances of the service are allocated to each customer. In this way, each user has its own dedicated resources and independent allocation. In the multi-tenant model, one instance of the service is accessed by multiple users; a single instance allocates the same resources to all customers or to a group of customers, and these resources are divided into portions where each customer has exclusive access. Multi-tenancy can be achieved through several technical means[34], one of the most prominent being virtualization[35]. The multi-tenant model is more lightweight, but its risk is that, since a single instance of the service is shared among multiple users, data pertaining to, or stored by, one user could be accessed by other users of the same instance. This could lead to issues such as personal data breaches or, if a user stores data covered by intellectual property, to violation of intellectual property rights. It is therefore important that each customer is able to access exclusively his or her reserved area; the assets of a customer must not mingle with those of others[36].

2.2. *The cloud in business*

Cloud computing comes in two different paradigms[37] involving two or three stakeholders, depending on which of two different models are in place:

- business-to-customer (B2C)[38];
- business-to-business (B2B)[39].

In its essence, the former case entails a simple contract between the Cloud Service Provider (CSP) and the end-user. A business provides cloud-based services to end-users. In this configuration, the business is the cloud itself. This form is generally used for simpler architectures, where the vendor offers some software in the form of services and hosts the cloud itself.

The B2B configuration is based on two or more separate and independent relationships: at its simplest, one between the CSP and the enterprise customer, and another between the enterprise customer and the end-user. In short, users access services

[31] However, in general, contracts with CSPs often contain some liability waiver clauses. These clauses can impose strong limitations on users' rights, and they might not be valid in all jurisdictions. The topic is widely covered, e.g., Bradshaw, Millard, and Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services"; Calloway, "Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm"; Kafeza, Kafeza, and Panas, "Contracts in Cloud Computing." See also *infra* at Section 4.3.

[32] Azeez et al., "Multi-Tenant SOA Middleware for Cloud Computing."

[33] Kwok and Mohindra, "Resource Calculations with Constraints, and Placement of Tenants and Instances for Multi-Tenant SaaS Applications."

[34] For an overview, see Krebs, Momm, and Kounev, "Architectural Concerns in Multi-Tenant SaaS Applications."

[35] Virtualization is a technique in which a software replicates the functionality of a complete hardware machine, using all or part of the resources of the (physical) machine on which the software is run. By leveraging on the fact that a virtual machine generally does not use all the resources of the physical machine, by running multiple virtual machines on the same physical machine it is possible that multiple users operate on the same hardware but in logically-separated spaces. The individual user might have no knowledge of working on a virtual machine instead of a physical one. For more details on virtualization, see Barham et al., "Xen and the Art of Virtualization."

[36] Bezemer and Zaidman, "Multi-Tenant SaaS Applications: Maintenance Dream or Nightmare?"

[37] However, it should be noted that the distinction is not extremely sharp, as it is quite common that a B2C application can also be used in a B2B context. See Dinh et al., "A Survey of Mobile Cloud Computing" for a detailed analysis of the various classifications of cloud computing.

[38] Just to name one of the thousands of B2C platforms available, a very popular example would be Google Docs.

[39] Again, there are plenty of B2B applications available, especially in the financial sector. A paramount example of a cloud B2B service is Salesforce.com.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

through tools provided by a vendor, but these services rely on resources on a cloud provided by an external CSP. What with their structural features, the PaaS and IaaS delivery models are normally oriented at the B2B configuration, where the cloud offers enterprises an environment where their applications will be hosted and executed. In theory, there is no significant technical difference between the two models[40], as the CSP might provide the same services to an individual or a legal person. However, there are significant differences from a legal perspective, both concerning the structure of the relationship and the consequent liability.

In its simplest form, the CSP provides a cloud. The CSP offers facilities and services to use the cloud, either as a platform for enterprise applications, or for direct use by end-users. From the perspective of the software vendor, the B2B paradigm consists of outsourcing its software to the CSP. Some authors[41] refer to this as "cloudsourcing".

Whether the software vendor provides its own cloud or it relies on an external CSP, however, the perspective from the end-user is the same, and it is drastically different from the traditional software approach. Typically, the end-user of a cloud-based software no longer owns a standalone physical copy of the software. The end-user generally owns the physical copy of some software code (front-end), if any at all[42], which cannot be used unless an access to the cloud is available. This reflects the move from an economy centered on goods (the standalone software product distributed by means of the sale of its physical support coupled with the software license) to one centered on services (where the enterprise does not offer the software but a service which provides the software functionality).

3. Property of the cloud

When viewing the perspective of property of the cloud, the protection granted to it differs depending on what facet is examined[43].

Of course, the physical components on which the cloud runs can benefit from ordinary protection of material goods. In modern systems, however, it is quite likely that cloud services do not rely on physical equipment, whereupon other, lower-level cloud services provide the hardware resources needed. Ultimately, some physical equipment must lie at the basis of the stack of interconnected services, but control of it might well be beyond the reach of the provider of higher-level services. Hence, a cloud service might or might not be subject to the protection of material goods, depending on whether or not there is any equipment susceptible of physical apprehension.

If the physical components of the cloud belong to the enterprise running the service, property can be viewed on two different levels: the level of the individual component (e.g., the single rack blade, or the warehouse where the servers are stored), and the level of their collection. Only when assembled and managed as a whole the components are able to form the cloud. This corresponds to the legal concept of *universality*. The following sections will briefly cover the complex topic of universalities, and the implications of such a view of the cloud.

3.1. *Universalities*

It is widely recognized that property, and therefore trade, may concern individual things or sets of things. Material things can be grouped into other things that can be themselves the object of ownership. When things are grouped, they may form either a *composite thing*, if the individual components lose their significance as separate tradable goods (such as what can happen, roughly speaking, to the parts that make up a car), or a *universality*, if they keep having an autonomous function (for example, the books in a library). In a universality, the individual things do not actually form a new thing, but they do so only in trade[44]. In other words, they make up a collective good only to the extent that they are traded as such, or when the law defines them as a unity (such as the patrimony in a succession, or estate in common law terms).

The concept of universality, or *collection of goods*, or *aggregate of things* (depending on the actual source)[45] refers to a set of goods and rights that have an individual tradability, but also make up a distinct collective good with a unitary purpose, and can itself be the object of a contract. The concept originates from late Roman law, and it was known as *universitas facti*; however, significant differences exist between the Roman *universitas* and the modern universality: the former represented a legal person, ultimately corresponding to a foundation, whereas the universality is not a personified entity in modern legislation, but only an object subject to a special regime.

In modern law, the universality appears in the legislation of several civil law countries, generally in the contexts of foundation and succession. The existence of the concept emerges in the civil codes of France and Luxembourg as *universalité des biens* (art. 1003 in both cases, concerning successions), and of Spain as *universalidad de bienes* (art. 600, on servitudes). The civil codes of Portugal (art. 206) and Brazil (art. 90) have a more detailed definition of *universalidade de fato* as "a plurality of movable things that, belonging to the same person, have a unitary purpose". The same definition appears in the Italian civil code (art. 816) for the *universalità di mobili*; additionally, Italy has specific provisions addressing the acquisition by prescription of

[40] This is clearly an approximation. In practice, a CSP catering to end-users will generally offer a final, standalone service (typical examples are travel agencies or cloud storage services), while a CSP serving enterprises will provide an infrastructure on which its customers can deploy their services. The distinction will be better explained in Section 2.1 *supra*.

[41] Géczy, Izumi, and Hasida, "Cloudsourcing: Managing Cloud Adoption."

[42] While PaaS and IaaS clouds often make use of some front-end to provide their functionality, this is generally not the case in SaaS clouds, where access to the service is made plainly through an Internet browser.

[43] For a detailed analysis of the regulatory framework of software in general, see Dusollier, "Electrifying the Fence: The Legal Protection of Technological Measures for Protecting Copyright."

[44] See, for example, Yiannopoulos, "Introduction to the Law of Things: Louisiana and Comparative Law," 783.

[45] The concept does not have a uniform name in English, since it is not native to the legislation of English-speaking countries.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

a collection. The civil code of Venezuela does not define the *universalidad*, but it contains specific provisions concerning universalities in articles 782 and 794 (on possession), 834 (on testaments) and 1433 (on donations). The German civil code refers either to the *Inbegriff von Gegenständen* (§ 260) or *Inbegriff von Sachen* (§§ 92 and 1035)[46], although in German doctrine the term *Sachgesamtheit* is used as well[47]. In addition to the civil code, other laws in Germany contain provisions specifically for universalities: *Gesetz über den Versicherungsvertrag* (Insurance Contract Act 2008), § 89[48], or § 54 in the repealed act. In the United States, the concept is recognized in the civil law State of Louisiana[49]. Legislation and jurisprudence of the European Union occasionally refer to the collection of assets as well[50].

Traditionally, and in legislation, the concept of universality is limited in the type of things that it can contain: a universality is made up of tangible (corporeal), movable goods. However, the concept has been expanded to also include rights and obligations. For example, this applies to the patrimony (or estate) of a person, especially for the purposes of succession and taxation. The *universitas iuris* is recognized in several countries: the *universalità di diritto* in Italy, elaborated by doctrine and jurisprudence[51]; the *Rechtsgesamtheit* in Germany[52]; the *universalidade de direito* in Brazil (art. 91 of the civil code)[53]; the *universalidad jurídica* in Mexico[54]; and the *universidad de derecho* in Venezuela[55] and Chile[56].

A particular type of universality is the firm, which is a well-known concept in civil law systems. A firm is the collection of assets (storage buildings, offices, wares, machines, vehicles, documents) that jointly contribute to perform business activities. In other words, it is made up of a set of individual goods, whose collective functionality is determined by the business owner. Despite being made up of a collection of goods, the firm is also a good of its own. However, the firm is not a legal person, but only the set of assets that are used by a natural or legal person to conduct a business, or a branch thereof. This concept closely corresponds to that of universality, although the firm has some peculiarities that generally do not belong to universalities in a strict sense. First, a firm can also contain immovable things, such as warehouses or terrains, whereas legislative definitions only embrace movable things. Secondly, the owner of a firm might not own the property of every individual component, whereas a universality is generally a set of things belonging to the same person in terms of property. In a firm, for example, some immovable things or machines might be used for business purposes on the basis of a lease contract. In spite of these differences, the dominant doctrine is not discouraged from accepting the qualification of the firm as a universality through an extensive interpretation[57].

In general, individual business assets can be the object of contracts. Alternatively, a collection or aggregate of assets (a firm, in particular) can be traded as a whole[58]. In the latter case, the consequences depend on what exactly the assets of the firm are, henceforth what is the object of the contract.

Even the theory of the firm as a collection of assets does not exhaust the debate. The advocates of the firm as a universality are divided between the two different perspectives of a *universitas facti* and a *universitas iuris*. According to some commentators, for example in the U.S.[59], Germany[60], France[61],

[46] Möller and Sieg, *Kommentar Zum Versicherungsvertragsgesetz Und Allgemeine Versicherungsbedingungen Unter Einschluß Des Versicherungsvermittlerrechts*, 2:270.

[47] Wieling, *Sachenrecht*.

[48] "Insurance taken out for an aggregate of items covers each individual item belonging to the aggregate of items. If the insurance is taken out for an aggregate of items, it covers the items belonging to those persons with whom the policyholder is sharing a common household upon occurrence of the insured event or who are employed by the policyholder at that time and are working at a location covered by the insurance. The insurance shall thus be deemed to have been taken out for the account of a third party." See also Marlow et al., *Das Neue VVG Kompakt: Ein Handbuch Für Die Rechtspraxis*, 276; Johannsen, "§ 89 Versicherung Für Inbegriff von Sachen."

[49] Supreme Court of Louisiana, *In Re: Howard Marshall Charitable Remainder Annuity Trust*, 13.

[50] Article 5(1) of Council Regulation No 1346/2000; Article 21(1) of Directive 2001/24/EC; Article 5(8) of Sixth Directive 77/388/EEC. The Court of Justice refers to the collection of assets (or set of assets): see Court of Justice of the European Union, *TETS Haskovo*; Court of Justice of the European Union, *X*.

[51] Bianca, *La Proprietà*.

[52] Wieling, *Sachenrecht*, 1:61.

[53] de Matos, Varela, and de Lima, *Código Civil Anotado*, I:199–201.

[54] Rojina Villegas, *Bienes, Derechos Reales y Sucesiones*.

[55] Oscar and Ochoa *Bienes y Derechos Reales*, II:9–10.

[56] Silva Segura, *Acciones, Actos y Contratos Sobre Cuota: El Problema Jurídico y Práctico de Las Acciones y Derechos*.

[57] This view is well-known in civil law systems. See, for example, Colombo, *Il Trasferimemto [Sic] Dell'azienda e Il Passaggio Dei Crediti e Dei Debiti*. According to Fairén Guillén and Gómez Colomer, *Estudios Sobre La Ley de Enjuiciamiento Civil y Su Práctica Inicial*, in Spain the theory of the firm as a collection of assets can be inferred from article 592 of the civil procedural code. However, such a view has also reached common law countries. American doctrine has recognized the firm as the collection of assets owned by a business: see for example Garrouste and Saussier, "Looking for a Theory of the Firm: Future Challenges"; Garrouste, "The New Property Rights Theory of the Firm"; Moore, "The Firm as a Collection of Assets"; Grossman and Hart, "The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration." As shown by Berle, "The Theory of Enterprise Entity," U.S. courts have applied the theory of a firm as a collection of assets to affirm the presence of a company where no legal entity exists.

[58] Several examples exist in civil law countries. French legislation allows contracts concerning business assets (*fonds de commerce*) as a whole (French *Code de commerce*, articles L141-1 through L144-13), including sale (*acte de vente*, articles L141-1 through L141-32), pledge (*nantissement*, articles L142-1 through L142-5) and lease (*location-gérance*, articles L144-1 through L144-13). The German civil code does not have specific norms for the sale of business assets (*Betriebsvermögen*), but the objective is achieved through the application of §§ 433, 413, 929 and 873 of the German civil code. In Italy, the sale of a firm follows the ordinary rules for the sale of a collection of assets, with additional provisions (artt. 2557–2560 of the Italian civil code) concerning the credits and debts of the business.Also common law countries such as the United Kingdom recognize the acquisition of assets. For instance, legislation addresses tax issues and labor law for the preservation of employees' contracts.

[59] Moore, "The Firm as a Collection of Assets"; Hart and Moore, "Property Rights and the Nature of the Firm."

[60] Möller and Sieg, *Kommentar Zum Versicherungsvertragsgesetz Und Allgemeine Versicherungsbedingungen Unter Einschluß Des Versicherungsvermittlerrechts*, 2:270.

[61] Satanowsky, "Nature juridique de l'entreprise et du fonds de commerce."

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

and Chile[62], the firm is considered as a *universitas facti*, made up only of things (physical properties). Other theories, such as in Italy[63] and Germany[64], interpret the firm as a *universitas iuris*, comprising not only physical goods but also a set of rights and obligations. Both theories are supported by plenty of doctrine and jurisprudence, and the qualification of the firm also differs from country to country.

These two visions have a major difference with respect to what a firm actually encompasses. If the firm is a universality of things, then it is made up only of those physical things, whether or not they are a property of the firm's owner, which are used to perform the business activity. This perspective does not consider contracts, credits and obligations to be part of the firm as such. On the opposite, the firm as a *universitas iuris* also comprises rights and obligations, including credits and contractual positions.

3.2. *The cloud as a universality*

Materially speaking, the cloud is made up of a set of technological assets. It is partly composed of physical goods: the computers on which the software runs and the data is stored; the wiring, network switches, racks to create a physical infrastructure; the storage rooms and cooling systems which make up the environment they are located in. The software that runs the cloud environment is an asset in itself. There are additional software programs, such as the operating systems, drivers, management tools, networking programs, which are required to run the systems. These might have been developed in-house, or licensed from external suppliers. The technology might also rely on patents, both software and hardware, which could belong to the CSP itself or be supplied under license.

In addition to the above goods, the cloud might rely on contracts, such as electricity supply, hardware maintenance, insurance or consulting.

From a strictly civil perspective, all of the above make up a *collection* (or *aggregate*) *of indefinite assets*, both tangible (the hardware architectures and storage facilities) and intangible (software, protocols, patented technologies and so on). Under a different perspective, the cloud can be viewed as (part of[65]) a firm, as it represents part of the assets that are required to perform the business activity. These two perspectives do not collide, based on the aforementioned theories according to which a firm is a collection of assets (a universality).

Such a qualification has important consequences, especially concerning the effect of deeds or events that transfer the ownership of the cloud (e.g., sale contracts or the death of its owner), but these consequences are not uniform. Significant differences may emerge depending on whether the property of the cloud belongs to a single natural person, it is in co-ownership among a number of natural persons, or it belongs to a legal entity. Consequences may also differ according to applicable national law.

An *inter vivos* deed[66] to transfer a business offering cloud services will have different effects depending on the applicable law and the legal nature of the firm. In particular, in legal systems familiar with the concept of universality, a deed certainly transfers all physical assets, such as computers and servers, network and cabling equipment, the physical facilities where the equipment is stored, and so on, which are required for the cloud services to work[67]. Concerning non-physical assets such as software licenses, patents, author's rights, databases, and so on, the matter is more complex, depending on the view of the firm as a *universitas iuris* or *facti*.

Intellectual property is not identical to physical property. It is a complex set of rights allowing economic exploitation of the intellectual property, either through usage or through lease and licenses. For this reason, it can be part of a *universitas iuris*, but arguably not always of a *universitas facti*. Therefore, the legal nature of the firm, as described above, has significant implications on whether the firm in itself also contains intellectual property rights. More specifically, as a *universitas facti* only includes goods (both material and immaterial), all owned intellectual property is part of it, whereas the intellectual property used on the basis of a contract (e.g., a license) is not. Therefore, if the cloud is seen as a *universitas facti*, then leasing and licenses for intellectual property are not included in the transfer, and separate contracts (regulated by the specific regimes of each asset) are needed to transfer them[68]. Conversely, if the cloud is seen as a *universitas iuris*, the contracts concerning intellectual property rights are part of it and are therefore included in the transfer[69].

Whether the transfer of the firm should also include intellectual property is up to the contractors and the purpose of the transfer. If the purpose is that of a business continuity, then the transfer should also include all the intellectual property rights required to offer the service. On the other hand, if the purpose is to dismiss the business, then it is up to the parties to determine whether to include those rights in the transfer,

[62] Adriasola Navarrete, *La Transformación de La Empresa*, 43–44.

[63] The firm is qualified as a collection of things, rights and obligations in Ferrara and Corsi, *Gli Imprenditori e Le Società*; *Cass. civ. 8219/1990*.

[64] Epping, *Die Aussenwirtschaftsfreiheit*, 76–79; Bundesgerichtshof (Zivilsachen), *Urt. v. 07.06.1990, Az.: III ZR 74/88: Puffreisriegel*.

[65] The cloud may constitute the whole of an enterprise's business (in which case the cloud is the firm), or just a branch of its business (in which case it is a subset of the firm).

[66] The most obvious example is the sale of the cloud from one owner to another, but it can also be the effect of corporate actions such as the acquisition or split-up of the company owning the cloud.

[67] Special rules might apply for specific categories of goods, such as immovable things and real estate used as storage facilities, so that the sale of a firm might require specific contractual clauses in case such goods are included in the firm. Additionally, in most countries the transfer of immovable things is recorded in public records. When transferring the firm as a whole, real estate included in the firm will be subject to the appropriate form of publicity.

[68] It should be noted, however, that this also depends on the nationality of the business and its applicable law. For example, whereas in France the firm is seen as a *universitas facti* (see Satanowsky, "Nature juridique de l'entreprise et du fonds de commerce"), its transfer also includes all the intellectual property rights connected to the firm, including licensed ones (French *code de commerce*, article L142-2). Under the same legislation, some intellectual property rights cannot be transferred unless the firm is transferred as well (e.g., French *code de la propriété intellectuelle*, article L623-22-2).

[69] In this case, specific clauses or contracts might be needed in case the parties want to prevent licensed intellectual property to be transferred along with the cloud, remaining with the seller instead.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

or exclude them. Since the legal nature of the firm (and therefore of the cloud) is uncertain, the contracting parties should specify which intangible assets they plan to transfer[70].

3.3. *The cloud as intellectual property*

The material goods, even collectively, are not sufficient to provide cloud services. For this purpose, they must execute software programs that provide the desired functionality. Additionally, the overall setup of the components, the way the services are presented to end-users, the logical interconnection between the various services, and even marketing elements such as the logo and the brand name all contribute to making up the cloud. All these elements of the cloud are, in different ways, the product of human intellect, and not suited for material apprehension. Therefore, depending on their nature and purpose, each of them is subject to legal protection as intellectual property (IP).

In other words, the cloud is *also* a collection of intellectual property assets. However, intellectual property is not subject to ordinary private law rules, for example concerning transfer and lease. Possession of property in general is sufficient to guarantee the exclusive usability of a good. When applied to industrial assets, this means that the owner, or the legitimate user on the basis of a contract, of the (physical) assets has the exclusive right to use them, and this exclusivity is guaranteed because the assets are in his or her material relationship with the goods. This is in itself a protection of the enterprise's investments. The problem with intellectual property is that it is not susceptible of physical apprehension[71], so that the exclusive right to use intellectual property assets cannot be guaranteed by their material impossibility to be used by more than one person at the same time. What is more, intellectual property consists of concepts, ideas, and in general creations of intellect that may circulate through knowledge or information, and therefore anybody possessing such knowledge could theoretically use it. This would be detrimental to the enterprise, whose investments to achieve certain assets would not be rewarded by the exclusivity of their use. Consequently, the protection against third parties must follow a different approach, normally through a legal regime that forbids anybody who is not entitled to use such assets, and imposes penalties for infringements of the prohibition[72].

The difficulty in dealing with the topic is that intellectual property rights (IPRs) are not a homogeneous concept, but rather a set of protection measures that operate collectively, and in general have the nature of *prohibitions*. If a piece of intellectual property is protected for single use by an enterprise, then no one else is entitled to use it, even if by some means (legal or not) they have access to it. This work does not aim at investigating deeply the huge issues of intellectual property, so it will only provide some significant points that are particularly relevant for cloud computing.

3.3.1. *Copyright protection*

The business approach to software has caused some confusion in the past[73]. In particular, it was unclear to most users that they did not "own" the software, but were only entitled to use it according to a license. Intellectual property is inherently more complex to grasp than estate property. Owners of a physical copy of the software were inclined to think that it was actually in their right to do whatever they wanted with it, including making copies and redistributing it. Even when aware of the exact boundaries of their rights, the ease of replicating a copy of the software at no cost, coupled with the technological developments that made copying materials cheaper, was often an incentive to redistribute software, thus breaching the license[74]. This situation has led to a significant evolution in the software market, characterized on one side by the constant struggle by software vendors to develop protection systems that would hamper the redistribution of their software, and on the other side by a high degree of software piracy and means of countering the anti-piracy measures[75].

The gradual shift toward distributed architectures and cloud computing drastically changed this scenario. A significant amount of modern software does not follow the traditional paradigm. Rather, end-users obtain a software that is not self-sufficient to execute the desired functionality. It can either be a full-fledged application that requires access to data that is

[70] In cases where the property of the cloud does not belong to a company but to a single natural person, or is co-owned by a plurality of natural persons, since the cloud is also part of its owner's estate, the owned share will fall into the person's succession upon the owner's death and be the object of a *mortis causa* transmission. However, the consequences of such a situation are not uniform and depend on factors such as the place where the owner dies and the location of the cloud assets, since succession is regulated by national laws.

[71] Hughes, "The Philosophy of Intellectual Property."

[72] Computer software, and digitalization in general, strongly influenced the landscape of intellectual property law, because they introduced the easy circulation of intellectual property independently from the need of a physical means. See Radin, "Information Tangibility." However, some aspects of the very same landscape changed again with the expansion of cloud computing, as software moves from an economy of products to an economy of services.

[73] See Section 2 *supra* for a description of the passage from a model similar to the sale of goods to one more resembling the provisioning of services.

[74] Katz, "A Network Effects Perspective on Software Piracy" essentially contradicts the classical thesis, supported by anti-piracy advocates, that software piracy is detrimental to producers. According to the author, by benefiting from a "network effect", software piracy can effectively increase the diffusion of a software, thus imposing *de facto* monopolies, technological lock-ins, and a barrier against new competitors.

[75] Software piracy was a major problem in the 90's and early 2000's. An analysis of the impact of software piracy on the industry is proposed by Givon, Mahajan, and Muller, "Software Piracy: Estimation of Lost Sales and the Impact on Software Diffusion." A paramount victim of software piracy, whose products still circulate illegally, has been Adobe Systems Inc. (see, for example, Kin Wai Lau, "An Empirical Study of Software Piracy"; Muchmore, *Stolen Software: Piracy Hits More than Movies and Music*). It has even been reported by Foss, *Will Software Piracy Fears Keep Adobe Products out of China?* that Adobe was close to dropping out of the Chinese market because the localization of its software cost more than the expected revenues due to piracy.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

not stored within the user's computer[76]; or a thin client that simply provides access to features that are implemented in a remote service[77], as in the typical SaaS delivery model. The complete appliance is usable only in connection with the cloud resources, which are under the control of the software vendor. The cloud resources can be maintained either directly by the vendor (in-house cloud) or via a contract with a third-party CSP.

This is a strong disincentive to software piracy: redistributing the software by means of unauthorized copies does not provide any benefit to the recipients, because the availability of the software is not sufficient *per se* to exploit the functionality of the service[78].

By empowering the vendor with a full control over who accesses the cloud-based resources, cloud computing offers a partial solution to the problem of piracy. Naturally, at present the traditional software approach, where software is distributed in a standalone form that resides completely on the customer's machine, cannot be completely replaced by cloud-based software. There are many situations, especially in enterprises, where security and reliability issues demand software that is totally available internally, and cloud services are not a viable solution.

The design, the structure, and in general the software making up the cloud service is subject to copyright protection[79]. It is a form of protection based on a knit framework of national and supranational laws, international treaties, and conventions[80]. In short, there are three different levels of legislation for copyright protection. The first one is based on international treaties and conventions, starting with the Berne Convention[81] (and other minor ones), which was embraced by the World Trade Organization (WTO) in 1994 with the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs). The second level distinguishes two macro-models of copyright law: the common law model, based on the protection of the publisher's rights to distribute a work, and the civil law model, centered on the protection of the author's rights[82]. The third level is that of national legislation, where countries (and in particular EU Member States) have a limited freedom of regulating copyright within the boundaries set by international treaties and conventions and supranational laws.

In general, software, as a product of the intellect, is subject to copyright protection, concerning both the source code and the way it is presented to users[83]. Although the Berne Convention does not explicitly address software, its protection stems from the national legislation of most countries, and (in the European Union) from an *ad hoc* Directive[84], which, being specifically related to computer programs, also affects cloud services. This Directive does not create an autonomous right, but provides a special application of copyright protection, extending the application of the Berne Convention to computer programs[85]. The protection covers "only the expression of a computer program", whereas the "ideas and principles which underlie any element of a program, including those which underlie its interfaces, are not protected by copyright"[86].

The Directive has a twofold purpose. First, to create a balance between the rights of the author of the computer program to prevent its unauthorized reproduction[87] or alteration on one side, and the rights of licensees to obtain information that

[76] This configuration can be driven by technical requirements and not just business choices: in some cases, the application cannot provide its full functionality because the data is too volatile to store them locally, for example in case of news readers or stock trading services. In other situations, the data is mainly static but simply too big to be entirely delivered to the end-user, such as in the case of world maps and satellite images.

[77] Typical examples are cloud storage services, which simply provide an interface that allows the user to store and retrieve his or her data in a cloud environment.

[78] Not even this assertion is totally true. Even if the software vendor does not make available some parts of the assets to the end-user, it is sometimes possible to replicate them and set up an environment independent from the vendor. This phenomenon has become quite popular over the last decade in (non-free) online gaming platforms, where private illegal servers (called *shards*) are quite common and sometimes host large communities of users. A description of the phenomenon can be found in Debeauvais and Nardi, "A Qualitative Study of Ragnarök Online Private Servers: In-Game Sociological Issues."

[79] However, it should be noted that the degree to which software is subject to copyright law has been a subject of significant debates. The attitude toward the copyright protection of software has been ebbing and flowing over the years. Menell, "An Analysis of the Scope of Copyright Protection for Application Programs" presents an early analysis of copyright protection of software, identifying a first stage in which the protection concerned the exact copy of the software, and a second stage in which the courts judged infringements more widely, also encompassing the look and feel and the general sequence of operations. Jurisprudence has tried to trace the line between what is copyrightable and what is not. For an example in the United States, expressly Mattel, Inc. v. MGA Entertainment, Inc., 616 F.3d: "Designs, processes, computer programs and formulae are concrete, unlike ideas, which are ephemeral and often reflect bursts of inspiration that exist only in the mind." According to Graham and Mowery, "Intellectual Property Protection in the U.S. Software Industry," U.S. enterprises resorted to a larger use of software patents in response to a decline in the copyright protection of software. See also Bessen and Hunt, "An Empirical Look at Software Patents." For the difficulties of dealing with computer programs in copyright protection and an overview of other forms of IP protection for them, see Christie, "Designing Appropriate Protection for Computer Programs."

[80] For a detailed insight, see for example Ginsburg and Treppoz, *International Copyright Law*.

[81] Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886.

[82] The distance between the two models is significantly reduced after the TRIPs agreement. In particular, a legislation framework exists within the European Union, concerning copyright in IT systems, to which the United Kingdom cleaves as well. The bulk of the EU legislation is contained in Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, with a constellation of other Directives concerning minor aspects. In contrast, the United States are subject to the Copyright Act of 1976, in addition to other legal sources, among which is notably the Digital Millennium Copyright Act of 1998.

[83] But see *supra* at note 87.

[84] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.

[85] Ibid., Article 1.1.

[86] Ibid., Recital 11.

[87] Ibid., Recital 13.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

guarantee the interoperability with other computer programs[88] on the other. Second, to harmonize Member States' legislation regarding the protection of computer programs, providing the legal environment necessary to guarantee the security against unauthorized reproduction of such programs[89].

From a general point of view, it has been observed[90] that traditional copyright protection shows several weaknesses when applied to software, and a *sui generis* right might be more suited. The reason behind this is the dual nature of the software, which exists both in the forms of source code and machine code[91]. The former is human-readable, and can be reasonably compared to a literary work, and therefore undoubtedly subject to copyright protection. The latter is the form that, after the source code is processed by *ad hoc* programs called *compilers* or *interpreters*, is suitable for computer execution. It is not human-readable, it is generated by the combination of the source code and the compiler or interpreter (so that different compilers could translate the same source code into different versions of machine code), and it pertains more to the functionality of the software than to its expression. This dual nature already introduces some impediments to copyright law, because the very definition of "software" is ambiguous: if software is intended as the set of instructions required to perform a task, then it only refers to machine code. However, the possibility to protect machine code under copyright law has been fluctuating[92]. Other problems arise from the fact that, in order to run a software, the computer must necessarily perform one or more copies of it in its internal memory.

However, in the context of cloud computing, copyright protection of the service *per se* is not a major issue. Since the Internet greatly increased the ease of replicating software code[93], the online service paradigm lying at the basis of cloud services has helped protection against software piracy[94], as cloud-based software does not need to circulate to be used. In any case, the functionality of most cloud services can be replicated with ease, even without having access to the software code or without the need to imitate the layout of the service. The real vantage point of a cloud service does not lie in the software code running it, but in its popularity and user base.

3.3.2. *Database protection*

A specific regime that integrates copyright protection is the legal protection of databases[95]. As cloud services often rely on large amounts of data, which may even be the only source of revenues in their business model, this protection has a significant importance in clouds. In some cases[96], it is even possible that a database is the only content of the cloud service[97].

At the European level, database protection is offered by a specific Directive[98], which goes beyond the copyright protection of a database, as the latter is based solely on the criterion of *originality*[99]. In other words, only those databases that sport a particular structure or arrangement that can be considered as a product of the intellectual work of the author are eligible for copyright protection[100]. Indeed, databases that meet the originality requirements would be protected under copyright law even in the absence of the Directive; however, as it has been observed, Member States might define different criteria to qualify a database as original, and the Directive harmonizes the rule[101].

If a database does not qualify for copyright protection, then it is protected by a *sui generis* right[102] in case it involves a qualitatively and/or quantitatively substantial investment by the enterprise in the obtaining, verification or presentation of its contents. Hence, the maker of the database has the right to prevent extraction and/or re-utilization of the whole or of a substantial part, from a qualitative or quantitative point of view, of the contents of that database. Protection lasts for ten years from first making the database available to the public, or fifteen

[88] Ibid., Recital 15.
[89] Ibid., Recital 4.
[90] Diver, "Would the Current Ambiguities within the Legal Protection of Software Be Solved by the Creation of a Sui Generis Property Right for Computer Programs?"
[91] For a detailed reconstruction of the problem, see Samuelson, "CONTU Revisited: The Case against Copyright Protection for Computer Programs in Machine-Readable Form."
[92] For an analysis of the early problems with the copyright protection of software see Stern, "Another Look At Copyright Protection of Software: Did the 1980 Act Do Anything For Object Code?" See also note 86 *supra*. The matter is in reality more complex than outlined here, as U.S. decisions have shown. Initially, copyright protection was afforded under very extensive terms to the structure of the software (except for those parts that are strictly necessary to perform its functionality), as in the landmark case of *Whelan v. Jaslow*, 797 F.2d. Later, the copyright protection of "non-literal elements" of the software was slightly relaxed, when *Computer Associates v. Altai*, 982 F.2d introduced a three-step test to assess whether a non-literal element should be subject to protection. For a detailed reconstruction, see Rowland, Kohl, and Charlesworth, *Information Technology Law*, 364–70; Lemley, "Convergence in the Law of Software Copyright."
[93] Widely recognized argument, e.g., Hinduja, "Correlates of Internet Software Piracy"; Meurer, "Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works."
[94] Ojala, "Software-as-a-Service Revenue Models."
[95] A database is defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Directive 96/9/EC, Article 1.2; see *infra* at note 80). According to the interpretation of the Court of Justice of the European Union, arranging the materials in a systematic way represents the added value of the database. See for example Court of Justice of the European Union, *Verlag Esterbauer*.
[96] For example, https://cloud.oracle.com/database (visited March 23, 2017).
[97] Soat, *Why Cloud Databases Are In Your Future*: "A database cloud service, or database as a service (DBaaS), makes database capabilities available online, when and where those capabilities are needed. The user can access a slice of a database (a schema), or, more likely, a complete, dedicated database instance. Or an enterprise can offer DBaaS running in its own data center for internal customers."
[98] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[99] Ibid., Recital 16.
[100] Ibid., Article 3.1.
[101] Rowland, Kohl, and Charlesworth, *Information Technology Law*, 387.
[102] Directive 96/9/EC, Article 7.1.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

years from its creation[103]. The Directive does not define the remedies in case of infringement, but leaves them to Member States.

Both rights (database copyright and especially the *sui generis* database right) bring out issues when databases are hosted in the cloud infrastructure.

Despite the conveyed protection, the Database Directive is said to be still cemented on the conventional paradigm that databases have a fixed structure and location where one accumulates and stores data. Questions are raised while conjoining the *transferability* of conventional databases and the free *availability* of Big Data[104] (in case the data is free for others to use). But the ubiquitous and pervasive features of the cloud obfuscates the physical location of databases: the ability of cloud providers to transfer the stored databases across multiple countries entails a problem when dealing with different legal jurisdictions[105], i.e., when the cloud provider's infrastructure is located outside the EU[106]. Such scenarios could be enhanced by automated procedures for checking whether database rights are clearly defined and its jurisdiction specified to confirm the legal compliance[107] (such checks may include the location of the infrastructure provider using a location constraint mechanism) or even envisioning a *legal "localizational" solution* that includes an unconditional waiver as an alternative for scientific databases and/or for databases transferred across different jurisdictions outside the EU/EEA countries but respecting local laws[108].

Also, according to a report[109] at the European Parliament, the Directive "is an impediment to the development of a European data-driven economy" where in principle, end-users would be allowed to enjoy unrestricted use and reuse of datasets in a claimed free market economy and cloud environment. This conclusion, however, is not shared by some experts, who argue that the Directive registers no impediment to the growth of Europe's data-driven economy nor cloud[110].

It has been said that legal interoperability among multiple datasets from different sources can occur when the legal rights, terms, and conditions of databases from two or more sources are compatible and the data may be combined by any user without compromising the legal rights of any of the data sources used[111]. It includes as the following conditions: a) the conditions to use data are clear and readily determinable for each dataset; b) the legal conditions granted to use each dataset permits the creation and use of "combined and derivative products"; and c) end-users may lawfully get access and use each dataset without seeking permission from data creators. Legal interoperability in the cloud still seems a specter regarding the pre-date cloud legislation.

Much of the information in the form of a database placed in the cloud will be protected by the *sui generis* database right and database copyright. Nonetheless, these IP rights will cover only the database itself, without granting any IP rights over the information uploaded by the service providers using the database or by customers uploading their information onto it, or over third-party software used in conjunction with the database. For those, contractual terms and pre-existing IP rights still apply[112].

3.3.3. *Patents and trademarks*

Patent protection in the IT domain is somewhat problematic. The topic is approached from two different perspectives. While there is no argument against the patentability of computer technology in the sense of hardware, significant issues arise concerning patentability of software. The problem mainly concerns the different regime between the United States and the European Union. While the U.S. explicitly recognize

[103] For a detailed analysis of the Directive and its interpretation, see Rowland, Kohl, and Charlesworth, *Information Technology Law*, 388–92. The authors also highlight the controversy regarding "spin-off databases", i.e., those databases that are built only as a support for the main business of an enterprise. A notable example is a train timetable: the main business is running the trains, and the database offers a support for that activity. According to a minor doctrine, those databases should not be subject to protection. See also Derclaye, "Databases Sui Generis Right: Should We Adopt the Spin-Off Theory?"; Visser, "The Database Right and the Spin-off Theory."

[104] Corrales and Djemame, "A Brokering Framework for Assessing Legal Risks in Big Data and the Cloud."

[105] Article 11.1 of the Directive states that the database *sui generis* right shall apply to databases whose makers or right holders are nationals of a Member State or who have their habitual residence in the territory of the Community; Article 11.2 includes companies or firms, which have their principal place of business or central administration within the EU. It may happen that that servers are located in countries outside of the EU, and that databases can be reproduced in virtual machines. Hence there is a risk of potential cloud computing transactions.

[106] According to Reed, "Information in the Cloud," "US law provides no *sui generis* protection for databases which consist of factual information, and only limited copyright protection for any elements of creativity in a database's structure. Thus, if a database protected by EU database right is hosted on a US-located cloud server, the right will only be infringed if the acts of extraction or reutilization take place on the EU, rather than at the server. A similar though reverse problem arises if a database is hosted on an EU-located cloud server but acts of extraction or reutilization are undertaken by a person located in the US."

[107] Corrales and Djemame, "A Brokering Framework for Assessing Legal Risks in Big Data and the Cloud."

[108] Corrales and Djemame.

[109] Committee on Industry, Research and Energy and Committee on the Internal Market and Consumer Protection, *Report on Towards a Digital Single Market Act*.

[110] "Bringing together different datasets from different sources that perhaps have never been linked before and analysing the information does have the promise of delivering new insights and allowing for more informed decision making. There is no evidence to show that the existence of database rights protection serves as a barrier to this activity". See Connor, "Database Rights Are No 'Impediment' to Europe's Data-Driven Economy: A Legal Expert Explains How Robust Rights Support Innovation." The author also observes that, the Directive contains a number of exceptions, meaning that, even where copyright or database rights subsist in datasets, they do not consubstantiate an unjustified barrier to the development of Big Data projects.

[111] According to the GEO Data Sharing Task Force. The Group on Earth Observations (GEO) is a voluntary, legally non-binding partnership of Member States and Participating Organizations that seeks to promote human welfare in nine "societal benefit areas" through the Global Earth Observation System of Systems (GEOSS). It has settled data sharing principles and guidelines that encourage the full and open exchange of data, metadata and products. See *White Paper: Mechanisms to Share Data as Part of GEOSS Data-CORE*.

[112] Reed, "Information 'Ownership' in the Cloud," 11.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

software patents[113] as a means of protecting the intellectual properties of enterprises[114], currently software does not enjoy the same broad protection in the European Union[115].

The aforementioned approach is the one followed by the European Patent Convention (EPC)[116], which represents the main legislative source for patents in the European Union[117]. The fact that certain software can enjoy patent protection in the United States, but not necessarily in Europe, means that European enterprises may find it more difficult to expand in the U.S. market. They may find that the software on the basis of which they offer their services is already protected by a patent in the U.S. market. For U.S. enterprises, penetration of the European market with new software-based products may be easier in that respect. Software unpatentability may stimulate software houses to improve existing computer programs and deliver them as a service, together with additional functionalities. Consequently, SMEs that could not afford to pay the royalties of all the assets they need and that are covered by patents have an easier access to the market. At the same time, the absence of patent protection may limit the growth of enterprises that already operate in the market.

When translated to the domain of cloud computing, this dichotomy has a straightforward consequence. On one side, there is no doubt that innovations concerning the physical structure of the cloud systems running the services are protectable[118]. Conversely, software delivered through a grid or cloud infrastructure, typically based on the SaaS paradigm (but the same also applies for the PaaS and IaaS delivery models), may not be patentable in Europe, as far as they are considered computer programs "as such"[119]. In other words, the software or computer program must produce a "technical effect" in order to be considered for patent protection in the EU[120]. However, the position of the EPO has progressively moved and more and more inventions related to computer program have been successfully granted patent protection in the EU[121].

With the advent of cloud computing, there has been a "veritable gold rush to register trademarks to identify the respective companies' cloud computing goods and services"[122], as the cloud has the potential to give a mark a worldwide visibility. From a general point of view, trademark[123] protection is more limited than other forms of intellectual property protection: as it does not offer a monopoly to the trademark owner, anyone is entitled to create and market an identical product or service, as long as it is marketed and offered under a different name or brand[124]. However, as asserted *supra*,[125] in cloud computing the fame and popularity of a service play a major role in its commercial success, and incumbent cloud computing brands are nowadays at the heart of the business model in the digital industry[126].

The Trade Marks Directive[127] and the Trade Mark Regulation[128] regulate the domain at the European level. This reform package contains a wide range of innovations, including changes to the

[113] As covered in Layne-Farrar, "Defining Software Patents", software patents are one of those concepts for which even finding a definition is problematic.

[114] See Bessen and Hunt, "An Empirical Look at Software Patents" for an analysis of software patents in the U.S.

[115] Although a detailed analysis of the debate is outside the scope of this work, the possibility of introducing software patents in the European Union has been the subject of a major controversy and a long political discussion. For a summary of the evolution of the topic, see Pila, "Software Patents, Separation of Powers, and Failed Syllogisms"; Leifeld and Haunss, "Political Discourse Networks and the Conflict over Software Patents in Europe."

[116] Convention on the Grant of European Patents (European Patent Convention) of 5 October 1973.

[117] Generally speaking, patents are regulated by the Paris Convention for the Protection of Industrial Property of 1883. However, pursuant to Article 19 of the Paris Convention, members of the Convention are allowed to make special agreements, not in contrast with the Convention itself, for the protection of industrial property. The EPC is regarded as one such agreement. See Muir, Brandi-Dohrn, and Gruber, *European Patent Law*.

[118] Parrilli, "Software Patentability in a Grid Environment", although focused more on grid computing than on the cloud.

[119] EPC, Article 52(2) and (3).

[120] European Patent Organization (EPO) Guidelines, Part G, Chapter II, para 3.6, which refers to European Patent Office, *T 1173/97 (Computer Program Product/IBM)*. See also the landmark Decision of the European Patent Office, *T 0208/84 (Computer-Related Invention/VICOM)*., which established that programs controlling or carrying out a technical process are not to be regarded as programs as such, and therefore not objectionable (para. 15 of the judgment) under Article 52(2) of the EPC.

[121] Since European Patent Office, *T 0208/84 (Computer-Related Invention/VICOM)* (see *supra* note 93), patent applications linking software to a technical process/effect have been largely successful. For a more thorough discussion of the topic see MacQueen et al., *Contemporary Intellectual Property*, 534–56.

[122] *Brand Protection for Cloud Computing*.

[123] According to the definition offered by Article 2 of the Trade Marks Directive (see *infra*), "[a] trade mark may consist of any signs, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, provided that such signs are capable of: (a) distinguishing the goods or services of one undertaking from those of other undertakings; and (b) being represented on the register in a manner which enables the competent authorities and the public to determine the clear and precise subject matter of the protection afforded to its proprietor". The definition is similar to the one contained in the U.S. Code, Title 15, § 1127, with two notable differences. First, U.S. law distinguishes between a trademark and a service mark, while no such distinction exists in European acts. Second, in U.S. law there is a *bona fide* requirement for a trademark to be defined as such, whereas European legislation does not require *bona fide* to qualify a trademark.

[124] Steier, "Legally Speaking."

[125] Section 3.3.1.

[126] As an additional argument to the renewed importance of trademarks protection in cloud computing, Weckström, "Trademarks in New Markets: Simple Infringement or Cause for Evaluation?" observes that "trademarks are not limited in time. This feature makes them more like real property (land) than other forms of intellectual property that are inherently limited in time. Consequently, trade mark protection suffers less harm in practice than other intellectual property".

[127] Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trademarks. Some parts of the Directive are not applicable yet, as they will apply starting 2019 (Article 56). Until then, the applicable provisions are those in Directive 2008/95/EC.

[128] Regulation (EU) 2015/2424 of the European Parliament and of the Council of 16 December 2015 amending Council Regulation (EC) No 207/2009 on the Community trade mark and Commission Regulation (EC) No 2868/95 implementing Council Regulation (EC) No 40/94 on the Community trade mark, and repealing Commission Regulation (EC) No 2869/95 on the fees payable to the Office for Harmonization in the Internal Market (Trade Marks and Designs).

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

fee structure, criteria concerning the eligibility for registration of trademarks and procedural issues, as well as certain changes applicable to infringement proceedings and customs seizures.

4. Property in the cloud

As complex and interconnected as the legal regime governing the physical and intellectual property of the cloud assets may seem, the problems that it raises are dwarfed by those that concern the data that is stored in the cloud by its customers. This is partly due to the extremely heterogeneous nature of the types and purposes of cloud providers, and correspondingly of the data that is stored in them. Other key issues (distinction between data and metadata; distinction between data stored by the user and data generated by the cloud service on the basis of the user's data; different contractual weights between the cloud provider and its customers; protection of personal data) significantly contribute to making the framework extremely problematic.

This section addresses the legal topics that are most relevant for the data stored in the cloud.

4.1. *Data ownership and copyright protection*

Who owns the data in the cloud[129]? The concept of ownership implies that of the owner's responsibility on how the data will be managed and regulated. In cloud computing, the problem of the ownership of data mingles with that of the distinction between data created by the user and by the cloud service. As cloud services create new data (e.g., statistical data, thumbnails of pictures, and so on), it is questionable whether such data, when generated through the processing of user data (or metadata) should be considered in the ownership of the user or the cloud service.

Another distinction, which does not correspond to the previous one, is that between data and metadata. However, in the context of this paper the distinction between data and metadata is irrelevant, because of the fact that a certain piece of information qualifies as data or metadata does not affect its ownership. Both data and metadata can be generated either by the user or by the cloud service provider. Furthermore, intellectual property rights do not behave differently on the basis of the distinction between data and metadata, but apply according to the type of information. It is also generally acknowledged that metadata should not benefit from a lesser degree of protection than data[130].

Normal copyright rules apply. If the data being stored in the cloud is fit for copyright protection (i.e., it has some degree of novelty and is the product of the author's intellectual work), the Berne Convention states that the author's right over the work comes into existence immediately as the work is created and without any formalities. Therefore, the user of the cloud service can have the author's right over the work or not, depending on whether he or she is the author. These rules will also apply to information placed in the cloud by service providers, third-party software developers, and database proprietors[131]. However, the cloud terms of service may include provisions according to which the cloud provider has some power over the data stored in the cloud. In other words, by accepting a cloud service's terms of service, it is possible that the cloud user agrees to grant the cloud service provider some power over the material published in the cloud[132]. This is not an actual copyright transfer, but depending on what the terms of service state, the author might be limited in exercising his or her monopolistic rights over the copyrighted material[133]. Ownership of IP can be eroded by a formal assignment of ownership or dedication of the work to the public domain; but in the cloud computing environment, the mere uploading of information to a cloud platform or service does not entail losing IPRs over the information[134].

Additionally, as cloud consumers retain IPRs over their own data, the cloud service provider will hold exclusive ownership over the rights used in providing the cloud service, i.e., it owns the IPRs to the software, and the customer will be granted a license to use the technology. Nevertheless, this should be made explicit in the terms of service, or negotiated in the contract with the cloud customer[135]. In the PaaS and IaaS delivery models, separation of ownership for applications developed by the cloud customers and the tools used to develop them should be made clear in the contract terms[136].

Furthermore, information placed in the cloud by customers may be protected by a database right, depending on whether the customer is responsible for the arrangement and layout of the data or the cloud provider offers specific templates for arranging and structuring the content[137].

[129] See Djemame et al., "Legal Issues in Clouds."

[130] See for example Guild and Carrera, "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive." The Court of Justice of the European Union reached the same result in Court of Justice of the European Union, *Joined Decisions C-203/15 and C-698/15, ECLI:EU:C:2016:970: Judgment of the Court*, and Bradley-Schmieg and Jones, *CJEU Confirms That National Data Retention Laws May Only Be Adopted Where "Strictly Necessary"* for a commentary to the decision.

[131] Cheung and Weber, *Privacy and Legal Issues in Cloud Computing*, 142–43.

[132] An old version of the Google Terms of Service (https://tools.google.com/dlpage/res/webmmf/en/eula.html, visited April 12, 2017), at article 11, stated: "By submitting, posting or displaying the content you give Google a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through, the Services". For newer versions of the terms, see Section 4.3 *infra*.

[133] De Filippi, "Law of the Cloud."

[134] Reed, "Information 'Ownership' in the Cloud," 6–7. For a more detailed analysis of contractual clauses, see Section 4.3 *infra*.

[135] Noble Foster, "Navigating through the Fog of Cloud Computing Contracts," 14.

[136] "First Study of Legal and Regulatory Aspects of Cloud Computing," 162.

[137] The Japanese government is taking a first step toward the introduction of a new form of intellectual property protection for Big Data, but the terms of the new protection have not been defined yet. See "Intellectual Property Strategy Headquarters." Regardless of the exact result that this process will harness, it is of extreme importance as it shows the recognition of a need for a new approach to intellectual property rights in the age of Big Data.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

On the other hand, data generated through the manipulation or aggregation of users' data, depending on its nature, may be claimed as intellectual property rights by the cloud service. Examples of such data are advances in technology made using cloud consumer data, algorithms developed while optimizing the data of cloud consumers, or statistical analyses[138]. Such information is generally not owned by the users themselves as it is not provided by individual users, but is the result of the combination of information provided by a multitude of users, and this combination is performed by the cloud provider itself. If the provider discovers that displaying the data provided by users in a particular format provides a better user experience, that specific arrangement may be filed for patent protection (if applicable law permits it). Similarly, when the provider performs statistical analyses on data provided by users, the outcomes of the analyses depend not only on the samples selected but also on the operations of selecting the samples, the means of aggregating the data, of correlating data from different sources, and of displaying it. The latter part is an intellectual work that may deserve its own IPRs (such as copyright) in addition to the ones granted to the individual pieces of data[139].

At a higher level, it can be observed that the attempt to apply the classic legal concept of "ownership" to data gives rise to a plethora of problems that have a hard time finding their place in real estate or civil law categories. Whether data should be treated as property is a question that has not been clearly answered yet[140], and the complexity of the question is made worse by the heterogeneity of legal systems, which have different approaches to property, whereas the ease and speed of transferring data would call for a uniform legal regime. Given its subtleties and the range of complications to which the concept of "ownership" of the data gives rise, it may be preferable to outright avoid trying to identify an owner of the data, and rather switch the perspective to the prism of IPRs and responsibilities of each stakeholder[141].

4.2. *Liability for the content*

Even if the cloud provider is not entitled to IPRs over the material that its users store in the service, it does not mean that it is exempt from any accountability if said material is the ground for a civil or criminal offense. As the cloud provider offers a service in the IT context, it is subject to laws governing IT providers, and in particular, in the European Union, the so-called "E-Commerce Directive"[142]. The application of the Directive to cloud providers can be inferred by the interpretation of its provisions, although no decision by the Court of Justice expressly states that the Directive applies to cloud services.

The Directive applies to "information society services"[143], which are defined by a separate Directive[144] as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"[145]. Cloud services are offered "at a distance" (i.e., without the simultaneous presence of both parties), "by electronic means" (using equipment such as computers and other devices) and "at the individual request" (meaning that the cloud provider will not provide its services in the absence of a request by the user, as what occurs for example in broadcasting services)[146]. Additionally, since remuneration is a natural but not necessary element of the definition, cloud services that are free of charge still fit into the category. The application of the E-Commerce Directive to cloud providers holds regardless of the service delivery model: SaaS, PaaS and IaaS services, as well

[138] A useful taxonomy that classifies data according to its origin, although in reference to personal data, is provided by Abrams, "The Origins of Personal Data and Its Implications for Governance." However, that taxonomy can, to some extent, be used in this context for clarification. The author distinguishes between provided data (created by direct actions taken by the user), observed data (information that is observed and recorded), derived data (information generated mechanically by performing transformations or operations on other data), and inferred data (the product of a probability-based analytic process). Only the data belonging to the first category is information over which the provider cannot claim any rights, whereas the other three categories might qualify for ownership in favor of the provider (assuming the specific data meets the requirements of the various IP rights). Derived data, however, might still entail some shared ownership between the customer and the provider (the typical example is an automatic translation, which may qualify as a derived work in copyright law terminology).

[139] The topic of data ownership appears to be particularly delicate in such cases. For example, it has been argued that, when using social media for medical diagnosis, "the social media site operator as well as the provider and patient have an ownership stake in the data": Petersen and DeMuro, "Legal and Regulatory Considerations Associated with Use of Patient-Generated Health Data from Social Media and Mobile Health (MHealth) Devices."

[140] A positive answer appears to be implicitly given by Al-Khouri, "Data Ownership: Who Owns 'My Data'?" However, the author argues that when a user puts data online, he or she *delegates* the ownership, and afterwards the data has multiple owners. This answer is not satisfying from a legal perspective, because the concept of delegation of ownership is unclear, and the acquisition of property is governed by law and cannot be the consequence of an action to which the law does not attribute such an effect. A positive answer also seems to be implicitly given by Kaisler et al., "Big Data." As in the previous case, the article is written from an IT perspective, and does not aim at delving into the subtleties of the legal concept of property. The recent case of *Your Response Ltd v Datateam Business Media Ltd* (*EWCA Civ 281*) does not take an explicit position on the question whether data is property, but states that data is not property susceptible of a possessory lien. Again, this answer appears insufficient, because the same can be said of any type of intellectual property or immaterial goods. Many legal systems generally recognize that property and possession are not the same concept, and something that is not susceptible of material apprehension can still be the regarded as property.

[141] This thesis is close to the one expressed also by Evans, "Much Ado About Data Ownership." The author observes that the application of the concept of ownership, in the classic legal sense, to data is not a viable solution to deal with the problem of protecting the various rights associated with data.

[142] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

[143] Article 1.2.

[144] Article 2(a) of the E-Commerce Directive expressly refers to Directive 94/34/EC, as amended by Directive 98/48/EC.

[145] Directive 94/34/EC, Article 1.2.

[146] Annex V of Directive 98/48/EC provides examples of services that do not fit into the category of information society services, because they lack at least one of the three requirements.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

as the other, less popular types, meet the three requirements that classify them as information society services.

The main implication of the application of the E-Commerce Directive to cloud providers is that they are subject to the regime concerning the liability[147] of Internet intermediaries[148] for the information or content transmitted or stored by them on behalf of third parties[149]. For cloud services providers, the greatest risk in this context is that they may host or transmit information protected by intellectual property rights, notably copyright[150]. This may occur, for example, when clients store copies of copyright-protected materials (text, images, videos, music) on cloud servers, but also when they make this content available to other users or to the public without consent from the right holders. The matter may be complicated if the uploading client has played a part in the creation of the work, as is often the case with user-generated content (UGC). Copyright law is complex and has a number of so-called fair use exceptions under which the activity may be permitted, but these are not harmonized on a European level[151]. It may be difficult for a cloud provider to know exactly under which scenario users potentially violate copyright when uploading, recording[152], streaming, or sharing content on a cloud service platform.

Therefore the provider is exempt from liability for illegal or infringing content on its servers if the following two conditions apply: it has no part in determining the content of the transmission, or it has no knowledge or control of illegal information stored on its servers; and it acts expeditiously to remove or prevent further storage and transmission of any illegal information it is made aware of. The latter requirement is also referred to as a notice and takedown obligation[153].

These conditions may sound straightforward, however there has been controversy over when an information host has acquired that actual knowledge or control which makes him liable to act and remove infringing or illegal content. In *L'Oreal v. eBay* the CJEU determined that an information service provider may acquire such an active role, potentially causing secondary liability, where it optimizes or promotes content uploaded by its client[154]. In the same case it also confirmed that the defending information host eBay can be asked to take measures to prevent future infringements of the same kind as those previously ended under a notice and takedown procedure[155]. In addition, in the EU secondary liability may arise where the information service providers do not act as a diligent economic operator by failing to apply reasonable duties of care to detect and prevent illegal content on its platform[156]. It has to be noted, however, that the E-Commerce Directive does not require the provider to proactively monitor all information on its system in a general way for illegal or infringing activity or information[157]. How this squares up in practice to the requirement to act as a diligent economic operator is not entirely clear[158].

Host providers, especially in the B2C area, could put in place mechanisms, such as contact forms or addresses, enabling users to notify them of infringing content in order mitigate this risk. Subsequently, processes to review and remove any content found to be infringing or illegal would need to be put in place. To summarize, while host providers must react promptly to notifications of infringing activity or content, and may be asked to prevent repeat infringements of the same kind, this does not mean that they will have to monitor all traffic for illegal activity.

There are recent EU policy proposals in the area of copyright and hate speech which could limit the liability exemptions of host providers and mandate them to deploy technical

147 In the years before the Directive, some controversy had arisen on the liability of service providers. Most notable was a case occurred in Germany in May 1998, where Mr. Felix Somm, managing director of CompuServe, was found liable because some users of CompuServe services had hosted child pornography in newsgroups. The decision received a lot of attention, because, by applying ordinary German criminal law to service providers, it charged criminal liability on a manager for the behavior of a customer. For background information see also Mayer, "Europe and the Internet: The Old World and the New Medium"; Timofeeva, "Hate Speech Online: Restricted or Protected – Comparison of Regulations in the United States and Germany."

148 A detailed analysis of the topic from an official point of view is offered by Verbiest et al., "Study on the Liability of Internet Intermediaries"; "Legal Analysis of a Single Market for an Information Society: Liability of Online Intermediaries."

149 The Directive distinguishes between several types of information society services, depending on the type of service they provide. Services can fall under the categories of "mere conduit" (Article 12, if they solely offer a means for the recipient of the service to transmit information across a network), "caching" (Article 13, if they store information for the sole purpose of improving the efficiency of the transmission of information), and "hosting" (Article 14, in case they store information upon the request of the service recipient). For the most part, cloud providers fit into the third category, since they store the data submitted by the user. However, it is also possible that a cloud provider offers a caching or a mere conduit service (for example, in case of voice transmission).

150 Senftleben, "Breathing Space for Cloud-Based Business Models." There are additional complexities for services hosting hyperlinks or where linked content is embedded in websites. This article has a more detailed discussion of the matter.

151 Directive 2001/29/EC, Article 5 gives member states the option to apply certain exceptions and limitations for example for research purposes, satire and parody, criticism and review, or public security.

152 "BGH: Shift.Tv, Urteil v. 22.04.2009, Az. I ZR 216/06." For more detailed discussion of this judgment by the German Supreme Court see Senftleben, "Breathing Space for Cloud-Based Business Models," 91–92.

153 The exact conditions for such notifications and the removal of infringing content are not harmonized under EU law, and differ across Member States (if they are formulated at all). While infringing content needs to be removed, in practice the provider has the liberty to investigate the claims by the notifying party and refuse to remove the content if it finds no infringement. Contrary to U.S. law, a counter notice procedure (see *infra*) by the affected party, whose content is being removed, is not part of EU law.

154 Court of Justice of the European Union, *L'Oréal and Others,* para. 116.

155 Court of Justice of the European Union, para. 144.

156 Court of Justice of the European Union, paras. 120-124.

157 Directive 2000/31/EC, Article 15(1).

158 For a more detailed discussion of key CJEU rulings in this context see Valcke, Kuczerawy, and Ombelet, "Did the Romans Get It Right?"

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

measures in order to prevent and detect infringing or illegal content[159].

A similar regime of liability exemption exists in the United States. The Communication Decency Act of 1996 contains a provision[160] which is considered of primary importance to ensure freedom of speech on the Internet. The provision states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". The exemption from liability in this case is even stronger than that offered by the E-Commerce Directive in the European Union: the "notice and takedown" policy is not a legal requirement, but it may be enforced in court only in case it is expressly stated by the provider[161]. Courts have subsequently used this provision to deny any plaintiff's complaint against providers in case of defamatory statements by users[162]. There is little doubt that the section also applies to cloud providers, because its definition embraces providers of "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server"[163], and cloud providers offer their services by allowing users to access their servers.

On the other hand, the U.S. Digital Millennium Copyright Act of 2000 introduces stronger liability requirements on providers concerning copyright violations[164]. The section again states that the provider, in general, is not subject to liability for copyright infringement by its users, but also introduces some requirements[165] providers must comply with to be eligible for such exemptions. These conditions consist in the adoption and application of a policy for termination of the service against customers who repeatedly infringe copyright laws, and the absence of any interference with the technical measures used by the industry to protect copyrighted works[166]. Notice and takedown procedures in the DMCA are more prescriptive than in the E-Commerce Directive and they include an obligation for information hosts to allow for counter notices to be considered[167]. Counter notices are filed by content providers who argue that their content has been unjustly removed. Similar provisions exist in other countries, although the regimes differ slightly[168].

Broadly speaking, a general model exists throughout the world which grants service providers an exemption from liability, generally with the addition of a "notice and takedown" policy[169]. Due to the differences in the various regimes, the applicability of said regimes to cloud computing services must be evaluated on a case-by-case basis, depending on the provisions of the specific country and the nature of the service provided on the cloud.

In short, cloud providers (and particularly those in the EU and the U.S.) can generally benefit from all the liability exemptions generically offered to Internet service providers. These liability exemptions require the cloud provider to apply a "notice and takedown" policy (*ex lege* in the EU; when adopted on a voluntary basis, and *ex lege* against any violation of copyright, in the U.S.) according to which, upon notification, they must prevent any further violation or even terminate the infringing user's access to the service.

[159] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, COM(2016) 593 final, and Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities, COM(2016) 287 final. For a more thorough discussion of the proposals, see Frosio, "Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy"; European Copyright Society, *General Opinion on the EU Copyright Reform Package*, 2017.

[160] U.S. Code, Title 47, § 230.

[161] Fenno and Humphries, "Protection Under CDA § 230 and Responsibility for 'Development' of Third-Party Content."

[162] Ehrlich, "Communications Decency Act § 230." See also Solove and Schwarz, *Information Privacy Law*, 176–86.

[163] U.S. Code, § 230(f)(2).

[164] Digital Millennium Copyright Act, § 512.

[165] Digital Millennium Copyright Act, § 512(i).

[166] This provision has been criticized by Bretan, "Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA," who observes that in some cases the courts seem to have adopted decisions which hold service providers liable in the absence of a preemptive supervision of the content transmitted by users.

[167] Digital Millennium Copyright Act, § 512(c)(3) requires notifications among others to include detailed contact information of the complaining party, identification of the infringing works or materials, and a good faith statement by the submitter over the accuracy of the information. Counter notices are provided for in Digital Millennium Copyright Act, § 512(g)(3).

[168] For an analysis, see De Filippi and McCarthy, "Cloud Computing: Centralization and Data Sovereignty." For example, the Japanese Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Act No. 137 of November 30, 2001), at Article 3, excludes the civil and criminal liability of service providers, "unless where it is technically possible to take measures for preventing" the infringement, or "there is a reasonable ground to find that said relevant service provider could know the infringement". Article 3(2) also contains a provision that exclude the provider's liability in case it has taken measures to block the infringing communication. The law does not distinguish between copyright infringements and violations of different rights. However, according to the definitions in Article 2, this law seems to be applicable solely to those services that provide a communication facility, and therefore it might not be applicable to all cloud services. Similarly, Article 26 of the Singapore Electronic Transaction Act 2010 (Cap. 88), exempts service providers from civil and criminal liability, notwithstanding the obligation to comply with a removal order of infringing material issued by the law or a court (thus introducing an additional burden for the damaged party to obtain the removal). In this case, the applicability of the provision to cloud providers seems more grounded, since it "includes the automatic and temporary storage of the third-party material for the purpose of providing access". In Russia, Article 17(3) of the Law "On Information, Information Technologies, and Information Protection" (No. 149-FZ of 2006), contains an exemption from civil liability for those persons (not necessarily providers of Internet services) transferring or storing the information, as long as they are unaware of the unlawfulness thereof. See also Naumov and Amosova, "Providers' Liability."

[169] A detailed analysis of the liability of service providers in a comparative perspective is offered by Seng, "Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries"; Garrote Fernández-Díez, "Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights."

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

4.3. *Contractual terms and liability waivers in cloud computing*

The contours of the relationship between cloud providers and service users are most frequently defined in the terms of service, which may be couched in a Service Level Agreement (SLA). Contractual terms may vary significantly between providers, including those regarding information and rights ownership. This section discusses possible allocation of ownership rights in the terms of service of cloud providers.

Whether an enterprise is using off-the-shelf services from large cloud providers or custom offerings from smaller cloud providers, it is essential to scrutinize the applicable terms. The cloud customer has an interest in having SLAs negotiated and agreed upon, specific in terms and scope, bound to unambiguous metrics and comparable with SLAs from other vendors[170]. However, a significant limitation for the potential customer is the fact that cloud providers frequently offer shrewdly drafted standard contracts, laid out by the provider and balanced in its favor, with little or no bilateral opportunity to change the terms[171], normally allowing for a limited category of static and non-negotiable click-through SLAs (usually ranked as gold, silver, or bronze ranges)[172]. Either the cloud customer accepts the terms of service as a whole, or he or she forfeits the service altogether. This is often achieved by means of "click-wrap agreements"[173], which are drafted entirely by the provider, and any operation performed by the customer entails an implicit agreement of all the terms. Therefore the customer is not able to participate in the definition of the contractual clauses.

The enforceability of click-wrap agreements has long been the subject of debate and of numerous court decisions[174]. Concerning the European Union[175], their enforceability depends on the respect of the Unfair Terms Directive (UTD)[176]. Conversely, after an initial resistance to click-wrap agreements, U.S. courts have sported a growing tendency to enforce them[177].

Some of the clauses found in terms of service can collide with or conform to the ownership of the rights of the owner of the information, or introduce some limitation of liability[178]. In some cases, contractual terms allow the cloud supplier to unilaterally suspend the service provision without a specific motivation[179]. When the owner of the data stores it in the cloud service, this might have severe consequences, as he or she is prevented from accessing his or her own data, even though he or she retains the intellectual property over it.

Terms of service may go as far as including limitations to the user's ownership of the content stored in the cloud, availing the possibility to use the content supplied by the end-user at their discretion, including the deletion of the end-user's files[180]. Also, within social networks cloud service contracts, users agree to grant a global license for all content supplied to the cloud[181] (it is worth noting that the global transmission of intellectual property rights over future works varies from country to country). Although such clauses do not expressly imply a transfer of the intellectual property to the cloud provider, some may stand on the verge of a collision with copyright principles and data ownership[182].

Contractual clauses could determine the IP rights that the various players in the cloud relationship own, thus preventing issues of implied licenses or equitable assignments of IP rights. Clauses could also grant to the different players the licenses of IP rights: (i) the customer might use a licensed software whose IP rights are owned by the provider or third party; (ii) the provider, by processing information in which the customer owns IP rights, will also require a license; (iii) when a third-party software or data is made available, the rights owner is likely to have it licensed to the provider[183].

As further delved in Section 4.5, terms of service should define the obligations of confidentiality which each player owes to the others, including any sort of restrictions.

It is known that the cloud generates new types of information[184], and questions concerning information ownership arise. Data can be generated by the cloud provider using practices to process and produce information from its collection of customer data, such as data mining tool techniques, statistics, analytics, and so on, where there is potentially

[170] Padhy, Patra, and Satapathy, "SLAs in Cloud Systems: The Business Perspective."
[171] Eisner and Oram, "Clear Skies or Stormy Weather for Cloud Computing? Critical Privacy and Security Contracting Issues for Customers of Cloud Computing."
[172] Macías and Guitart, "Client Classification Policies for SLA Negotiation and Allocation in Shared Cloud Datacenters."
[173] Click-wrap agreements derive their name from the concept of shrink-wrap. In short, click-wrap agreements are a set of terms set forth by the vendor of the software or service, followed by the option for the user to accept the whole agreement with a single click. See Pistorius, "Shrink-Wrap and Click-Wrap Agreements." Click-wrap agreements are generally used for two main purposes: copyright transfer and limitation of liability. For an extensive analysis of click-wrap agreements, see for example Gatt, "Electronic Commerce – Click-Wrap Agreements: The Enforceability of Click-Wrap Agreements."
[174] For a partial list of decisions in the United States, see Naylor and Ritter, "French Judgment Condemning AOL Illustrates EU Consumer Protection Issues Facing U.S. Businesses Operating in Europe."
[175] Naylor and Ritter for a specific application.
[176] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[177] For a history of the evolution of click-wrap agreements in U.S. courts, see Founds, "Shrinkwrap and Clickwrap Agreements: 2B or Not 2B?"
[178] Bradshaw, Millard, and Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services."
[179] A number of terms of services contain the following clause: "We reserve the right to suspend or end the Services at any time, with or without cause, and with or without notice". See for example the terms of service for Overleaf (https://www.overleaf.com/legal, visited April 12, 2017).
[180] For example, "after a commercially reasonable period of time, Dropbox may delete any Customer Data" (Dropbox Business Agreement, Article 7.2).
[181] Facebook Statement of Rights and Responsibilities (https://www.facebook.com/legal/terms/update, visited April 12, 2017), Article 2.1: "you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it".
[182] See *supra* Section 4.1.
[183] Reed, "Information 'Ownership' in the Cloud."
[184] Reed, 9; Reed, 18–20.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

valuable information for both the end-users and cloud providers[185]. The terms of a contract should be able to clarify, in line with the legal rules of IP and confidentiality, who owns the processed and derived data in case of Big Data projects and applications[186]. For example, if the user consents (or grants a license) to this exploitation of (anonymous) derived information, the provider is compliant toward his legal obligation of confidentiality and IP.

Clauses regarding cloud disputes also can play an important role. As the use of global cloud services develops, it is likely that more customers will find themselves as parties in international disputes regarding services delivered to their desktop or mobile; but while the cloud is considered to be location-independent, legal remedies are not. The disparity between the technological progress and the legal quadrant for cloud computing emerges in the legal nature of the disputes and in the legal issues stemming from contractual conditions favoring the local jurisdiction, choice of law of the provider, issues of IP rights and ownership disputes. The current legal context tends to hamper access to justice and consumer protection, with a strong misbalance in negotiation power between cloud providers and customers[187]. Online dispute resolution (ODR)[188] is a method of resolving disputes using technology as a facilitator or as a "fourth party"[189] in the dispute. It includes online negotiation, mediation arbitration, double blind bidding, visual blind bidding and assisted negotiation. It also addresses the issues of IP rights and ownership disputes, with potential savings in time, costs, and human involvement. The acclaimed speed, low costs, flexibility, ease of access and privacy that ODR offers resonate both with cloud providers and customers. For this reason, it is perceived as a much more flexible environment compared to court procedure or alternative dispute resolution. Although the applicability of ODR to cloud disputes is currently under investigation[190], the ODR community prospectively claims that disputes that have occurred online should be resolved online[191] and that ODR is one of the possible mechanisms for redress in case of cloud provider–user disputes[192].

Clauses that must be dealt with when moving one's business to a cloud provider are liability waivers and liability limitations. The subject rests on the conflict between two opposite interests. On one side, the cloud customer would want that any risk is under his or her own control and that no significant damage occurs due to technical problems or misuse by the cloud service provider. On the other side, if the cloud provider were liable for any loss of data due to an imperfect implementation of its services, there would be a strong limitation to the deployment of cloud services, because the risk in running such a service would be too great[193].

For these reasons, it is quite common that the terms of service of a cloud provider contain some liability limitation or liability waiver clause[194] through which suppliers claim that they are not liable for irregularities concerning the access or performance of the service[195]. The content of such clauses, however, can vary widely, depending on the content of the service, on the delivery model, and especially on the target market, i.e., whether it caters to private users (B2C) or to enterprises (B2B)[196]. The terms might also include a list of issues for which the service provider disclaims liability, such as loss of data belonging to the customer, damages to the physical equipment, security breaches, unfair behavior, denial of service attacks, and so on[197]. Liability waivers are particularly dangerous for the customer, because the customer can be exposed

[185] See also *supra* at Section 4.1.

[186] Corrales and Djemame, "A Brokering Framework for Assessing Legal Risks in Big Data and the Cloud."

[187] For example, according to Martic, "Online Dispute Resolution for Cloud Computing Services," an "SME from Indonesia, using SaaS paying 100 dollars per year, could have a dispute in front of California court and potentially pay approximately ten or twenty times more for fees and expenses, and then dependent on case backlog wait a while for the court deliberation on the issue."

[188] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR).

[189] Katsh and Rifkin, *Online Dispute Resolution*.

[190] Martic, "Redress for Free Internet Services under the Scope of the EU and UNCITRAL's ODR Regulations"; Martic, "Online Dispute Resolution for Cloud Computing Services"; Martic, "Dispute Resolution for Cloud Services: Access to Justice and Fairness in Cloud-Based Low-Value Online Services."

[191] See Rule, *Online Dispute Resolution for Business*; Abdel Wahab, Katsh, and Rainey, *Online Dispute Resolution*.

[192] See again Martic, "Online Dispute Resolution for Cloud Computing Services."

[193] A particular case of potential damages to the cloud customer is the one that occurs in case of a non-forewarned shutdown of the cloud service, or in case of bankruptcy of the cloud provider. This problem concerns the fact that the cloud customer might find itself unable to offer its service due to the shutdown of the cloud provider, adding to the fact that the data stored on the cloud service might not be accessible anymore, losing a long record of significant data. The problem and its potential solutions, both from a technical and a legal perspective, have been extensively analyzed in a previous work by the authors: Bartolini et al., "Cloud Providers Viability: How to Address It from an IT and Legal Perspective?"

[194] Dropbox Business Agreement (https://www.dropbox.com/privacy#business_agreement, visited April 12, 2017), Article 10.b: "Limitation on Amount of Liability. TO THE FULLEST EXTENT PERMITTED BY LAW, DROPBOX'S AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL NOT EXCEED THE LESSER OF $100,000 OR THE AMOUNT PAID BY THE CUSTOMER FOR THE SERVICES HEREUNDER DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY".

[195] Google Terms of Service (https://www.google.com/intl/en/policies/terms/, visited April 12, 2017.): "SOME JURISDICTIONS PROVIDE FOR CERTAIN WARRANTIES, LIKE THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. TO THE EXTENT PERMITTED BY LAW, WE EXCLUDE ALL WARRANTIES".

[196] For some considerations on possible features of liability limitations and waivers, see Parrilli, "Grid and Cloud Computing as a Tool to Transform European Economy: Legal Considerations."

[197] LinkedIn API Terms of Use (https://developer.linkedin.com/legal/api-terms-of-use, visited April 12, 2017), Article 12.3: "LINKEDIN DISCLAIMS ALL LIABILITY FOR ANY MALFUNCTIONING, IMPOSSIBILITY OF ACCESS, OR POOR USE CONDITIONS OF THE LINKEDIN APIS DUE TO INAPPROPRIATE EQUIPMENT, DISTURBANCES RELATED TO INTERNET SERVICE PROVIDERS, TO THE SATURATION OF THE INTERNET NETWORK, AND FOR ANY OTHER REASON". For an extensive analysis of the possible consequences of liability waiver clauses, see Calloway, "Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm."

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

to a number of factors that are not under his or her control (in addition to those that are), in particular a number of possible occurrences which may happen to the cloud provider. These sorts of clauses are considered unfair by the UTD.

4.4. *Vendor lock-ins*

Competition can be distorted in the domain of cloud computing, regardless of the delivery model that underlies the cloud. In general, there may be circumstances where data and application portability is not possible due to technical limitations or is prohibited by the service provider via contractual clauses. Such *vendor lock-in* effects may result in a distortion of the competition and an abuse of dominant position. Customers are locked into a firm's product or service when the costs or the disadvantages of switching a product or service are high, thereby discouraging customers to change [198].

There are several possible sources of vendor lock-ins. The "traditional" one (meaning that it is related to software in general and not specifically to cloud computing) consists of technical limitations that hamper the possibility of abandoning a provider. For example, the customer of a PaaS platform might be faced with the impossibility of porting an application and its data to another provider, if it was specifically tailored for the cloud environment on which it runs. When software is offered as a service (in the SaaS paradigm), harm to competition and consumers may result from data and application portability obstacles[199].

A second source of vendor lock-ins is tied to abusive licensing conditions placed by the platform provider on developers of applications (*apps*)[200]. Cloud computing has fostered the development of other platforms that introduce novel distribution models for digital content. These distribution models allow the controller of the distribution platform to provide services only to specific user devices. Such control gives a strong position in the market, which could result in the distortion of competition.

Vendor lock-ins can seriously hamper the circulation of the assets stored in the cloud. The owner of data or applications stored in the cloud does not have the possibility of easily moving them or taking back their control. Consequently, even transferring the assets can be a problem. For example, if an enterprise runs a service on a PaaS cloud platform and wants to transfer the service to another enterprise, which in turn is already offering other services through a different PaaS cloud, the recipient has to take into account the development costs to support the migration. The exit barriers of the first cloud might then lower the value of the sale[201].

The EU competition regime addresses anti-competitive agreements, abuse of dominant position and state aids.

In general, agreements, decisions of undertakings and concerted practices that have the object or effect of preventing, restricting or distorting competition and may affect trade between Member States are prohibited[202]. However, such agreements and practices may be exempted from the prohibition if they meet some requirements[203]. When applied to cloud computing[204], it may be difficult to prove the existence of one of the requirements, i.e., that the restrictions derived from the agreements are indispensable to the attainment of the agreement's objectives, due to the complexity contained therein.

Cloud computing is a fast-changing sector, and innovations may quickly change the market structure and erode the market share of the incumbent. Therefore, agreements and practices in an innovative sector are more likely to be exempted from the prohibition, as it may be difficult to predict whether substantial competition would be eliminated, and for how long an undertaking could manage to maintain a dominant position. Yet, network effects may allow not only to become dominant, but also to maintain the dominance for an extended period. Over time, such practices can distort competition and harm consumers by depriving them of better prices, wider choice, and innovation.

Abuse of dominant position by one or more undertakings is also prohibited[205], as an important tool for the Commission to protect and promote competition. If an undertaking is in a dominant position, the Commission may impose compulsory licensing of intellectual property rights on reasonable terms to avoid anticompetitive effects[206]. Additionally the Commission is willing to ensure that the intellectual properties of the dominant undertaking that result in market power and are essential for the development of new products are licensed and accessible to other market players in a fair, reasonable and

[198] See Walden and Luciano, "Ensuring Competition in the Clouds."

[199] The cloud provider might have an interest in enhancing network effects through the diffusion of its own products. Where network effects are operating, the market may support one firm's product or service, and it can become the *de facto* standard in the market, with the addition of intellectual property rights to protect it. For example, the notorious policy to "embrace, extend and exterminate" competitor products was often pursued by Microsoft, by adopting a public and widespread standard in its products, then introducing some proprietary additions to it, and finally binding customers to the extended proprietary version, thus killing the public standard in favor of the proprietary one. See for example Lee and Fulford, "Virtual Empires."

[200] This was the subject of recent investigations by the Commission in relation to Apple's iPhone applications. See European Commission, *Antitrust: Statement on Apple's iPhone Policy Changes*.

[201] Although not strictly related to cloud computing, the consequences of vendor lock-ins clearly emerged when Google shut down its Google Reader service, severely cutting down the RSS feed market. A large number of small businesses relied upon the service, either through news feeds or by developing services using the Google Reader API, and many of these were seriously damaged or forced to shut down after its sudden (but somehow expected) discontinuation. See Lehmann, *How Much Will Google Reader's Demise Cost Your Business?*

[202] TFEU, Article 101.

[203] TFEU, Article 101.3. First, they must "contribute to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit". Second, they cannot "impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives". Third, they must not allow the undertakings to "eliminat[e] competition in respect of a substantial part of the products in question".

[204] Cloud computing enterprises often rely on innovative agreements that benefit consumers in an economy of scale, so the first and third requirements for the exemption pursuant to Article 101.3 are generally met.

[205] TFEU, Article 102.

[206] E.g., Court of Justice of the European Union, *IMS Health*.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

non-discriminatory manner. As the market share threshold required under EU law for an undertaking to be considered dominant is 40%[207], in cloud computing (where network effects are higher) the non-applicability of competition law until a dominant position is attained could prejudice the goals of competition law[208]. As of yet, there are few Commission procedures pursuant to Article 102 and concerning cloud computing[209].

Article 107 prohibits a state from granting any form of aid that may distort competition by favoring a certain undertaking. As such, this prohibition may be relevant to cloud computing when a distortion to competition is caused by public administrations via public procurement decisions. Competitors excluded from the market may be able to complain and seek redress when, for example, a public administration chooses certain public procurement specifications which may lead to the elimination of a substantial part of competition[210].

The issue of vendor lock-ins might be mitigated by an important provision contained in the new European law for the protection of personal data, the General Data Protection Regulation (GDPR)[211]. In a nutshell, the right to data portability[212] allows a data subject (i.e., the person to which the personal data is related) to obtain the transfer of his or her personal data from one controller to another, and this right might apply in the majority of cloud services. However, as this is a new right introduced by the GDPR, its impact is hard to foresee. First, the GDPR shall apply from 25 May 2018[213], so that provision cannot be enforced yet. Second, the provision applies to personal data, and not to data protected by different forms of protection such as IPRs. Third, the scope of the provision also depends on the extent of the interpretation of the concept of "personal data".

4.5. *Trade secrets*

Trade secrets and know-how are covered under the umbrella of intellectual property. The TRIPs Agreement refers to "undisclosed information" to protect proprietary information, namely confidential information not covered by other intellectual property rights. Three requirements must be met for an information to be protected as a trade secret[214]. First, the information must be "secret in the sense that it is not [. . .] generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question". A second requirement is that the reason why the information has a commercial value must be that it is secret. Finally, the person interested in the information has a duty of taking adequate precautions, i.e., "reasonable steps [. . .] to keep it secret".

Trade secrecy laws are relevant for cloud computing. As the use of cloud services is becoming commonplace for enterprises, they store and access confidential information in the cloud[215]. Data stored in the cloud is located in third parties' remote data centers. While this leverages economies of scale and allows saving on storage costs, there are some risks involved if the documents stored in the cloud contain trade secret information.

Information stored in public clouds is potentially accessible to anyone with Internet access. Regardless of the extent of protection assured by the cloud provider, the protection of information is ultimately determined by the weakest link in the chain. Insofar as data is transferred through several intermediaries, only one of them needs to be violated for any malicious user to obtain relevant information[216]. How to safeguard a company's private data once it becomes part of an external computing network? Third-party cloud service providers (having custody of the data), and even company employees often pose the greatest threats to secrecy (sometimes because of a seemingly innocuous conduct).

The owner of the confidentiality right will not be affected by the act of placing the information in the cloud environment[217], as long as the provider and any others accessing the confidential information are under an obligation to maintain its confidence. However, cloud service providers sometimes may not have means of deciding which parts of the

[207] "Communication from the Commission: Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings," para. 14.

[208] Walden and Luciano, "Ensuring Competition in the Clouds."

[209] A notable example is offered by an infringement procedure against Google and concerning Android-powered devices. As Google services are strictly integrated among themselves (including services for Android devices), "Google obliges manufacturers, who wish to pre-install Google's app store for Android, Play Store, on their devices, to also pre-install Google Search, and set it as the default search provider", and also "to pre-install Google's Chrome browser". In other words, in order to provide their customers with services that are deemed essential for their products (Google's Play Store), device manufacturers are legally vendor-locked to include other services that are typically used by Google for advertising purposes. See also "Antitrust: Commission Sends Statement of Objections to Google on Android Operating System and Applications: Factsheet."

[210] See *Google, Inc. et al v. United States*.

[211] For a more detailed analysis, see Section 4.7 *infra*.

[212] GDPR, Article 20: "1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided [. . .]. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. [. . .]"

[213] GDPR, Article 99.2.

[214] TRIPs Agreement, Article 39.2.

[215] The protectable subject varies considerably from country to country. Commercial information, technical information, lists of suppliers and customers, and manufacturing and process secrets are among the denominations used by the Member States: *Report of the European Commission Conference of 29 June 2012 "Trade Secrets: Supporting Innovation, Protecting Know-How,"* 9.

[216] De Filippi and McCarthy, "Cloud Computing: Centralization and Data Sovereignty."

[217] As observed in Rashbaum, Borden, and Beaumont, "Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing," 85, "the Cloud customer, while not in physical possession of all of its ESI [Electronically Stored Information] all of the time, has the duty to preserve and produce such ESI. Accordingly, it is the practical responsibility of the Cloud Customer to secure vendors able to extract Cloud data and/or understand the CSP tools available for such data extraction when needed".

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

customer's information are confidential, nor will customers necessarily understand how far the information made available by the provider is confidential[218]. Yet, *"reasonable efforts"* to keep the material secret must create (at least implicitly) a duty of confidentiality. Such precautionary duty can be densified by contractual clauses[219]. Contractual terms may help in this sense by ensuring data ownership. The terms should clearly state that the ownership of user data stays with the user. The expression should be detailed enough to also avoid possible misunderstandings due to the difference in the legal context and the legal language of the cloud service provider and the customer, to prevent data from being lost or disclosed (e.g., in case a provider becomes a victim of acquisition or bankruptcy).

In order for businesses to obtain legal redress in court against the theft or misuse of their trade secrets, the new European Trade Secret Directive (ETSD)[220] aims at the creation of a safe and trustworthy environment for European enterprises.

Finally, the enterprise should use sufficient technical measures, such as encryption for the transmission of the data to and from the cloud, to ensure that confidentiality is not lost when the data is outside the control of the cloud provider.

If the necessary legal and technical means to maintain confidentiality are in place, then the third requirement for trade secret protection is not lost by storing data in the cloud. Additionally, under such conditions, the customer is protected by remedies for breach of contract in case the confidentiality obligation is violated.

4.6. *Export control*

If a cloud service allows users to store their own data in the cloud, additional restrictions might apply depending on the nature of the data being stored. One such regulation concerns national security, especially where weapons are concerned. Two main representative legal frameworks address this domain, one for the United States and one for the European Union[221], in addition to some international agreements. In the following, only a brief overview in connection with the specific topic of the present work will be provided.

The United States legal framework is mainly based on a Federal Act[222] and a Federal Regulation[223]. Its requirements are much stricter than the European ones. In particular, the ITAR regulations define any technical data pertaining to the U.S. Munitions List as a "defense article"[224], and cannot be exported to other countries, or made available to non-U.S. citizens or non-permanent residents of the U.S., unless a specific authorization is issued by the U.S. Government[225]. In short, this means that any software or technical data concerning military equipment should not be accessed by non-citizens or non-permanent residents.

The implications of such a regulation on a cloud service are quite strong. No data classified as a defense article should be stored on a cloud service whose headquarters are situated outside the United States, nor on a U.S.-based cloud service provider if the server where the data will be stored is located in another country, or if the route to store the data crosses other countries. Even if no communication outside the United States occurs, the cloud service provider would still be required to have some means of preventing access to non-U.S. citizens or non-permanent U.S. residents. In short, cloud services would need to be purposefully devised to store ITAR-classified software and data, with specific authorizations by the Government, otherwise such material could never be stored in them. Such a restrictive regime implies that enterprises and agencies dealing with ITAR material do not use cloud services, but rather non-public networks with strict access control policies.

The equivalent legislation of the European Union is somewhat similar to that of the United States. The core of the legislation is contained in one Regulation[226] (and several minor Regulations) and a Common Position[227]. In short, the scope of the European laws concerns "dual-use items", which are defined as "items, including software and technology, which can be used for both civil and military purposes"[228]. An extensive list of dual-use items is defined in Annex I of the Regulation, and the list includes technical data. The general rule is that dual-use items are subject to authorization prior to exporting. The concept of "export" also embraces "transmission of software or technology by electronic media, fax or telephone to a destination outside the Community". The Regulation appears to be slightly less restrictive than the ITAR, in that it does not expressly prevent any access from non-European citizens. However, given the fact that cloud service providers based outside the European Union, or with servers located in non-European countries, might be subject to a regime that is not compatible with the Regulation, storage of dual-use items (including technical data) in such cloud providers should be avoided in favor of private networks.

4.7. *Extraterritorial reach*

Once stored outside of the U.S. or the EU, national authorities may still try to re-gain access to the data outside of their jurisdictional reach, as can be witnessed from the recent Microsoft

[218] Cheung and Weber, *Privacy and Legal Issues in Cloud Computing*, 144.

[219] "The nature of cloud computing relationships would seem to suggest that the service provider impliedly undertakes to maintain confidence in the customer's information, and this may be stated expressly in the terms of service": in Reed, "Information 'Ownership' in the Cloud," 12.

[220] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[221] For a detailed analysis of the two legal frameworks and a comparison between them, see von der Dunk, "A European 'Equivalent' to United States Export Controls: European Law on the Control of International Trade in Dual-Use Space Technologies."

[222] Arms Export Control Act (AECA) of 1976, codified at the United States Code, Title 22, Chapter 39.

[223] International Traffic in Arms Regulations (ITAR), codified in the Code of Federal Regulations, Title 22, Chapter I, Subchapter M.

[224] ITAR § 121.1.

[225] Extensively, ITAR § 126.

[226] Council Regulation (EC) No 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology.

[227] Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment.

[228] Regulation 1334/2000, Article 2(a).

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

v. United States case[229]. In this case the U.S. Government, using the Stored Communications Act (SCA), tried to gain access to an email account hosted on Microsoft's cloud servers in Ireland. That claim was rejected by the judges because they denied the extraterritorial reach of the SCA. By contrast, in a more recent, similar case[230] in which Google was asked to provide user data stored on servers outside the U.S. under a SCA warrant, the California judges took on board the argument of the dissenting judges in the above Microsoft case. They argued that the warrant was a domestic application of the SCA since it was directed at the persons within Google's U.S. Headquarters who had access to the data in questions. It did therefore not matter where that data was stored[231]. Some commentators note that there is a trend by states worldwide toward extending extraterritorial jurisdiction when it comes to accessing content in the cloud[232]. In fact, countries across the globe have law enforcement procedures in place by which they can use the local facilities of cloud providers, be it offices or servers, in order to gain access to data stored outside of their jurisdiction[233]. Although this is usually done through court orders and search warrants, there is a tendency to avoid or bypass the more time-consuming and onerous mutual legal assistance agreements in this process[234].

The emerging extraterritorial approach also extends to data protection and personality rights, at least as concerns the EU. In its landmark case *Google Spain*[235], the CJEU ruled that the right to be forgotten needed to be enforced globally. It ordered Google to prevent the worldwide display of information held to infringe personality rights under EU law. The ruling was applied by the French data protection authorities in 2016, when they fined the American company EUR 100,000 for not complying with a global delisting request[236]. The original *Google Spain* case applied the 1995 EU Data Protection Directive[237] whose extraterritorial remit was contested[238]. The new GDPR however, which will fully replace the Directive by 25 May 2018, has a more defined geographic scope, which leaves little doubt about the fact that it will cover companies outside the EU if they process data of subjects located within the EU[239]. Meanwhile, intellectual property rights enforcement on the internet has also joined this trend with a recent decision by the Supreme Court of Canada[240]. In this case Google was enjoined to prevent the worldwide display of links on its search engine to websites of a company infringing the intellectual property rights of the claimant Equustek.

While not all of the above use cases related specifically to cloud providers, they highlight the general debate that is going on with regard to the reach of national courts relating to information displayed and hosted worldwide. The emerging tendency of governments to more proactively assert jurisdiction beyond their national borders in cyberspace has also been referred to as "hyper-territoriality"[241].

For cloud service providers this means they may in the future more often be confronted with requests by national authorities in countries where they have a physical presence (an office or a server) to provide or remove data based on their servers worldwide. Companies may therefore face more complex conflict of laws issues. Large service providers may have more resource and experience to address these than smaller or new players in the market.

4.8. *Protection of personal data*

Cloud computing services create also data protection risks, mainly a lack of control over personal data, as well as insufficient information concerning how, where and by whom data is processed and sub-processed[242]. The concept of processing of personal data is very broad[243], and likely to encompass most

[229] Microsoft Corp. v. United States, 829 F.3d.

[230] In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A, Document 45.

[231] In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A, Document 45 at 7–8.

[232] Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues," 475–78.

[233] Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues." According to this study, government authorities in Australia, Canada, Denmark, France, Ireland, Spain, the U.K. and the U.S. have powers to require local cloud providers to disclose data stored abroad.

[234] Daskal.

[235] Court of Justice of the European Union, *Google Spain*.

[236] Commission Nationale de l'Informatique et des Libertés (CNIL), *Right to Be Delisted: The CNIL Restricted Committee Imposes a €100,000 Fine on Google*. Google appealed the decision and the French court dealing with the appeal has referred the case to the CJEU, where it is currently pending.

[237] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[238] Keller, "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation."

[239] According to the GDPR, Article 3(2), the Regulation extends to entities outside the EU provided that two conditions apply simultaneously. One is a subjective condition, requiring that the processing concern personal data of EU subjects. The second is an objective condition, requiring that the processing activity relates to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

[240] Supreme Court of Canada, *Google Inc. v. Equustek Solutions Inc., 2017 SCC 34*.

[241] For a more detailed discussion, see Callamard, "Are Courts Re-Inventing Internet Regulation?"

[242] According to The European Consumer Organisation, *Putting an End to Silos in the Enforcement of Consumers' Rights*, "[t]he predominant internet business models is based on the monetisation and exploitation of consumers' personal data, often without consumers' knowledge or consent. This situation, coupled with the strong network effects that drive the digital ecosystem, is seriously undermining users' privacy and favouring the concentration of power in the hands of a handful of companies. Such overwhelming power allows companies to impose terms and conditions on users which they might not otherwise be willing to accept".

[243] GDPR, Article 4(2): "'processing' means any operation or set of operations performed upon personal information, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

of the operations that are likely to occur in the cloud, including the mere storage of data.

In cloud computing, enormous amounts of data can be gathered into large data centers, often interconnected. Information given to separate services can thus be aggregated together (either because the services are provided by a common cloud provider or through acquisition of data from third parties). Even though information had been voluntarily provided by users, aggregated data might provide further information about them, which they did not necessarily want to disclose[244]. Alleged concerns rely on the fact that integrating data from distinct sources encompassing personal information, even with apparently innocuous or anonymized data, may enhance a jigsaw of indirect identification and re-identification[245]. Another risk fueled by the processing of personal data in the cloud is the profiling of individuals[246]. The use of Big Data analytics, machine learning, natural language processing and data mining techniques may enhance the integration of personal data to create and use profiles[247].

The protection of personal data, especially at the level of the European Union, has been significantly evolving over the past decades. The current state of the art is the new General Data Protection Regulation (GDPR)[248], which builds over the developments of Member States, of the Council of Europe, and of the Charter of Fundamental Rights of the European Union.

Personal data raises significant problems concerning the data ownership. Being bits of information, of course, personal data is not subject to property in a real estate sense. However, in a broad sense, it can be said that personal data "belongs" to the data subject[249], who is the only person who can exercise the rights granted to him or her by the law[250]. No one else can exercise the data subject's rights, and no one else[251] is entitled to grant the consent for the processing of personal data. Even when the processing is not based on consent because carried out for the legitimate purposes of the controller or for public interests[252], the data subject still retains the exercise of the rights granted by Chapter III of the GDPR[253], unless specific derogations apply. Using legal categories, the data subject's rights are strictly personal legal conditions.

In personal data protection terminology, the controller is the person who determines the purposes and means of the processing of personal information[254], whereas the processor acts upon instructions from the controller[255]. However, these definitions are problematic when applied to cloud computing.

The cloud service provider normally qualifies as the processor[256]. In contrast, the controller is harder to identify in cloud computing, and depends on what data is stored and by whom. There are four types of data for which the answer to that question is different.

First, there is a set of personal data whose processing is based on the provider's decision, depending on the specific cloud (e.g., the data that is used to identify the user, or data explicitly requested by the cloud provider according to the service that it provides). The provider is definitely the controller with respect to such data.

The second set of personal data is composed of the information that the cloud customer autonomously decides to store on the cloud (e.g., in a cloud storage service such as Dropbox, the customer might decide to store a resume). To determine who the controller is with respect to such data, the GDPR can be interpreted in several possible ways, none of which is immune from criticism.

The first solution is that the cloud provider is again the controller, also for the personal data that the data subject decides to store. This reconstruction is possible if the definition of "controller"[257] is interpreted in the sense that, to be qualified

[244] De Filippi and McCarthy, "Cloud Computing: Centralization and Data Sovereignty." The risks of an uncontrolled processing of the personal data of persons have been repeatedly highlighted, e.g., see Zarsky, "'Mine Your Own Business!': Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion."

[245] This risk is described as re-identification from the aggregation of anonymized datasets. See further Article 29 Data Protection Working Party, "Opinion 7/2003 on the Re-Use of Public Sector Information and the Protection of Personal Data: Striking the Balance"; Article 29 Data Protection Working Party, "Opinion 03/2013 on Purpose Limitation"; Article 29 Data Protection Working Party, "Opinion 06/2013 on Open Data and Public Sector Information ('PSI') Reuse." The Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" presents a popular study that shows the ease of re-identification of the data subject by crossing personal data from different sources.

[246] Weber, "The Digital Future – A Challenge for Privacy?"

[247] Hildebrandt and Gutwirth, *Profiling the European Citizen*.

[248] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[249] GDPR, Article 4(1): the data subject is "an identified or identifiable natural person".

[250] Such as the right to a fair processing, the right of access, the right of opposition, the right to rectification, and in general all the rights granted in the domain of the protection of personal data.

[251] Except for the holder of parental responsibility in case of personal data of a child. See GDPR, Article 8.

[252] GDPR, Article 6.1.

[253] GDPR, Articles 12–23.

[254] GDPR, Article 4(7): "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

[255] GDPR, Article 4(8): "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

[256] There is a general consensus on this point. See for example Sotto, Treacy, and McLellan, "Privacy and Data Security Risks in Cloud Computing." However, some authors argue that in some cases the cloud service provider cannot even be considered a processor, as it only provides the customer with the means to process his or her own data. In other words, the processor would be the customer: see Hon, Millard, and Walden, "Who Is Responsible for 'Personal Data' in Cloud Computing?"

[257] According to GDPR, Article 4(7), the controller, "*alone or jointly with others*, determines the purposes and means of the processing of personal data" (italic added).

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

as a controller, it is not necessary to determine both the means and purposes of the processing, but determining the means is sufficient. It should be noted, however, that this interpretation does not appear to be followed by major institutions. On the contrary, the dominant interpretation is in the sense that the determination of the purpose is *per se* sufficient to qualify someone as the controller, whereas the determination of the means is not required to this end[258]. That said, if the arguable interpretation according to which the controller is the one determining the means only, and not the purposes, is followed, then, since the cloud service provider determines the means of the processing, it qualifies as a controller. The cloud service provider often makes important decisions about the means and conditions of processing personal information, such as where the information is stored, the use of sub-contractors and security. The problem of this perspective is to overly extend the accountability of the provider to any information, however sensitive (e.g., medical records or details on political affiliation), that the customer decides to store in the cloud, while relieving the customer of any liability.

Alternatively, as the customer would be the only one to decide the purposes of such processing, this would qualify him or her as the controller with respect to such data[259]. In such a situation, if the cloud customer is also a natural person, storing personal data pertaining to him or her, he or she would be the data subject and the controller at the same time, with the cloud provider acting as the processor in an intermediate position. However, the overlapping between the data subject and the controller would severely impair the European rules on data protection, because no one would be accountable as a controller, while the cloud service provider would have the more limited accountability of the processor.

The third possible interpretation is that in such a scenario there is no controller with respect to the personal data in this category, as there cannot be a coincidence between the data subject and the controller. This perspective achieves the same practical results as the one above, but its weakness is that, in the absence of a controller, the processor acts on behalf of no one.

Fourth, it can be argued that the real meaning of that expression "the purposes *and* means" in the definition of controller should be read as "the purposes *or* means" of the processing. In other words, both the customer and the provider would be controllers: the former because he or she determines the purposes[260], and the latter because it determines the means. Although this interpretation appears to efficiently accommodate the classic categories in the cloud environment, it requires to assume that Article 4(7) of the GDPR *minus dixit quam voluit*.

Finally, it is possible to view the cloud provider and the customer as joint controllers[261]. This solution has the benefit of finding a clear normative reference in the GDPR[262]. Its drawback is that, in the case of joint controllers, the respective responsibilities for compliance with the GDPR and the respective obligations (particularly concerning the rights of the data subject) should be determined "in a transparent manner" and "by means of an arrangement between them". However, it is unlikely that there is a clear arrangement (in the terms of service), for example to place some of the duties of information on the cloud customer[263].

What emerges is the difficulty of classic data protection categories to properly deal with cloud computing. The problem lies in the fact that the law does not contemplate the situation in which the purposes and the means are determined by different entities, except in the case of joint controllers which requires a prior determination of the responsibilities.

Although for the most part the above scenario does not have practical consequences on personal data protection (for example, a natural person processing his or her own data will not need to exercise a right of access to know what data is being processed and for what purposes), in cloud computing it can be extremely important to delimit the landscape of the cloud provider's accountability. Determining the exact responsibilities of the cloud provider with respect to this particular category of data may be especially problematic as the provider normally does not know the details of the data stored by the customer, whether it qualifies as personal data, or even special categories of personal data.

The third set of personal data concerns the information stored on the cloud by a user, but pertaining to a different data subject. This occurs very frequently in social networks, where users may upload personal data that pertains to other

[258] For example, the Article 29 Data Protection Working Party states that "while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means. In this perspective, it is well possible that the technical and organizational means are determined exclusively by the data processor." In Article 29 Data Protection Working Party, "Opinion 1/2010 on the Concepts of 'Controller' and 'Processor,'" 14.

[259] Although not explicitly stated, this seems to be the approach followed by the "ISO 27018" standard, although with a slightly different terminology: "[t]he cloud service customer, who has the contractual relationship with the public cloud PII processor, can [be] a natural person, a 'PII principal', processing his or her own PII [Personally Identifiable Information] in the cloud" (Art. 0.1).

[260] And, to a lesser extent, the means, at least with regard to the choice of the cloud provider. In this respect, the cloud customer could be liable on the basis of *culpa in eligendo*.

[261] GDPR, Article 26.

[262] This is essentially the interpretation followed by Buttarelli, *The Impact of the General Data Protection Regulation on Collaborative Science in Europe and the European Cloud Initiative*, according to which the user–provider relationship is that of "co-controllers, with shared responsibilities". Within this cognition, while the cloud costumer is the one deciding for what purposes data should be used, the cloud service provider decides how the infrastructure should be designed and how data should travel in that infrastructure. Together they make up the role of the controller. Of course, this opens up new questions about the individual responsibilities of each one. It should be pointed out that the GDPR has no reference whatsoever to the concept of "co-controllers", but the expression can probably be associated to the concept of joint controllers pursuant to Article 26.

[263] A "safety clause" in Article 26.1 allows Union or Member State law to determine the respective responsibilities. In the context of cloud computing, such a law that clearly states the responsibilities of the cloud provider and the cloud customer would be a significant aid in clarifying and protecting the data subjects' rights in cloud computing.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

individuals. Additionally, this scenario occurs when "bouncing" information from one cloud service to another[264]. Following the same line of thought as the previous scenario, it would be possible to assign the role of the controller to the storing user, to the cloud provider, or a combination of the two. In any case, the data subject would not be controller as well, and he or she might exercise remedies against the cloud user, the cloud provider, or both.

Fourth and finally, it is possible that the cloud provider generates statistics and other information by processing and aggregating personal data. Provided that these pieces of information do not allow re-identification of the data subjects, they must be considered an asset of the cloud provider and protected as intellectual property. Therefore they are a property (although not in a real estate meaning) of the cloud provider, and not relevant for the protection of personal data.

In the absence of a distinct definition of the roles in cloud computing, the exact role of the cloud provider needs to be assessed in each individual case, in order to appraise whether it must be considered a controller or not. If the partitioning of obligations and responsibilities between cloud customers and cloud service providers does not reflect their actual role within the cloud environment, there is a risk that no one takes full responsibility for the legal data protection obligations, and consequently insufficient protection might be awarded in real settings.

The GDPR might have introduced a significant breakthrough with respect to the concept of ownership of personal information. The combination of the right to erasure[265] and the right to data portability[266] theoretically allows the data subject a strong control over his or her personal data[267]. An effective application of these provisions would make the data subject the sole *dominus* of his or her personal data (unless some of the exemptions to Articles 17 and 20 apply), while the controller could not claim any ownership of such data. Some commentators[268] even argue that the GDPR introduces a property regime for personal data. The theory is based on three considerations: non-alienable entitlements of data subjects to their own personal information; the right to erasure that can be enforced *in re* rather than *in personam*, with an approach similar to the *ius sequelæ* typical of some real estate rights; and remedies that are similar to those grounded on property regimes. Apart from the second argument, which places too much emphasis on the right to erasure, the thesis appears to be correct. Personal data protection is indeed a regime that has many affinities with those of (intellectual) property. However, this does not seem to be a novelty introduced by the GDPR, as the classification of personal data protection in a relationship of *species* to the *genus* of intellectual property rights dates way back to the first steps in data protection[269].

Depending on the interpretation of the concept of personal data, the above effect might have a much wider scope. In a strict interpretation, "personal data" might denote only the information that directly pertains to the data subject. However, this concept might benefit from an extensive interpretation in the light of the new technologies and the means of profiling and identification using anonymized data. The huge processing capabilities of Big Data cloud providers are able to identify and draw a detailed profile of every data subject, even if apparently no name or unique identifier was provided[270]. In this new perspective, even data that does not directly allow the identification of an individual should be considered as personal data if such an identification is possible when combining that data with other sources. Possible examples are the recurring use of some specific expressions in a person's way of writing, ratings of mobile applications, the way of arranging folders on a hard drive, or reviews on hotels or movies[271]. Under an extensive interpretation of personal data, most of the information stored on the cloud by the customer might be considered personal data and fall under the protection of the GDPR and the scope of Articles 17 and 20[272].

Another unanswered issue is the *post mortem* destination of personal data in a cloud. The GDPR expressly avoids concerning data of a deceased person[273], and only a few Member State laws include provisions concerning the rights over the personal data of a deceased data subject. In the absence of a legal obligation to erase the data of a deceased person and of anyone able to exercise the data subject's rights, at the current state of things it can be assumed that personal data of deceased persons stored in a cloud service is relinquished and left at the mercy of the cloud provider.

The collection and processing of personal data is often regulated by contractual clauses, typically including implied consent, processing of personal data for secondary non-compatible purposes, and transfer of personal data in corporate mergers. The consent of the data subjects is one of the legitimate grounds for the collection and transfer of their personal information. For the consent to be valid, it needs to be specific, informed and free. Consent needs to be given in an unambiguous way, while a mere passive behavior does not suffice[274]. Data subjects need to be specifically informed about the data that will

[264] For example, a Twitter user posting a tweet that contains his or her own personal information falls under the second scenario above; however, a different user could share that tweet on Facebook. The question, then, concerns who is the controller with respect to the data uploaded to Facebook.

[265] GDPR, Article 17.

[266] GDPR, Article 20.

[267] The former is the right to obtain the complete erasure of all personal data under processing by the controller, while the latter allows the data subject to obtain his or her personal data in a structured format, allowing him or her to migrate such data to some different cloud provider. The right to data portability has been the object of some controversy in Swire and Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare," due to potential negative effects on security and competition.

[268] Victor, "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy."

[269] See for example De Sola Pool and Solomon, "Intellectual Property and Transborder Data Flows."

[270] See Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization."

[271] Ohm.

[272] See also the preliminary considerations on the right to data portability in Section 4.4 *supra*.

[273] GDPR, Recital 27.

[274] Article 29 Data Protection Working Party, "Opinion 15/2011 on the Definition of Consent."

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

be collected, the purposes and any third parties to whom the data might be transferred.

However, the privacy terms of many cloud computing service contracts are not transparent enough, do not disclose the necessary information to the users, and might not integrate all the legal requirements of the GDPR (such as the right of access or the right to data portability); they go as far as including vague terms referring to possible third parties to whom the data might be transferred without further clarification[275]. The terms are "take or leave", meaning that data subjects have no choice but to agree to such terms, otherwise they will not be able to use the service[276].

The GDPR does not provide for the case of a transfer of the assets (for example, the cloud provider selling some services to a different undertaking), a merger or acquisition, or a split-up (or division). However, adequate protection[277] should be granted to the data subjects[278], as such operations can seriously put personal data at stake. Several cases already have raised outcries concerning privacy risks, such as the merger between DoubleClick and Abacus in 1999. DoubleClick, a company placing advertisements online for its corporate clients, collected anonymized user data on the traffic generated by these advertisements. Abacus was a direct marketing company with an extensive database of consumer personal data. The merger, it was alleged, would have allowed the personal identification of online browsing behavior of the users tracked by DoubleClick. While a court case against DoubleClick merger was eventually dismissed[279], the FTC's investigation into unfair trading practices was also closed after assurances by DoubleClick that it would not merge its database with that of Abacus, and other commitments of DoubleClick regarding its privacy policies[280].

Meanwhile the more recent takeover of messaging service WhatsApp by Facebook is testimony that 15 years on concerns over the merger of user data gathered and managed online persist. Earlier in 2017, the EU Commission fined Facebook EUR 110 million for failing to inform it over the technical possibility of matching WhatsApp and Facebook user data[281]. The fine was imposed under competition law considerations relating to potentially incorrect information that may have affected the assessment of Facebook's market position after its merger with WhatsApp. While data and consumer protection did not play a role in the EU's decision, they highlight the legal challenges that a merger of company assets hosted in the cloud may entail. As regards data protection a German data protection agency has since denied Facebook the right to use WhatsApp data of its German users for the Facebook operations[282].

As personal data can constitute a significant part of a cloud provider's assets, its value should be accounted when evaluating the market value of the provider[283].

5. Conclusion

The changes that cloud computing brought along make it difficult to qualify it using traditional legal categories. Cloud computing is a modern paradigm that introduces a novel business model. On one side, it is now a well-developed model, resting on a consolidated common ground. On the other side, however, it is a multi-faceted world, with many different types of applications, each with its own peculiarities. In a situation where it is not possible to have a standardized and uniform legal regime for all possible needs, where can businesses and individuals look for appropriate protection? While cloud computing offers them many benefits, it is important to find the most suitable cloud solutions for one's applications and data. And unless the provider modifies its own offers, tailoring them to their specific requirements, the diversity and breadth of the cloud landscape makes it hard to match one's needs and the

[275] See, for example, the report on contractual clauses of cloud services "Hazy Terms in the Cloud: A Short Study of the Terms and Conditions of Cloud Storage Services."

[276] "That people continue to provide personal data and use services that collect data from them does not necessarily mean they are happy about how their data is used or simply indifferent. Many people may be resigned to a situation over which they feel they have no real control, but there is evidence of people's concerns about data use, and also of their desire to have more control over how their data is used." In "Big Data, Artificial Intelligence, Machine Learning and Data Protection," 27.

[277] In case of a merger or acquisition there are significant risks for the data subject, because his or her personal data might be processed by a controller that is different to the one to whom he or she gave consent, and also for different purposes. Ideally, a new consent should be requested, or at least the data subject should be informed about the merger and the purposes of the new controller, so as to exercise the right to object or to erasure.

[278] In the silence of the law, it is unclear what the adequacy requirements are. One solution is to apply the criteria for the transfer to third parties located outside the European Union. According to Directive 78/855/EC (Third Council Directive of 9 October 1978 based on Article 54(3)(g) of the Treaty concerning mergers of public limited liability companies), Article 19, "the *transfer* [. . .] to the acquiring company of all the assets and liabilities of the company being acquired" (italic added). As data can be considered an asset of the company, the merger would entail a transfer of the data. However, the GDPR only covers transfers to non-EU countries, whereas there is no requirement to transfer personal data within the European Union. An initiative in this direction was undertaken by the Italian data protection authority in Garante per la protezione dei dati personali, *Provisions Applying to Corporate Mergers and Split-Ups*. In particular, the Garante places a duty of information to data subjects and to the authority in case of a merger or division. It should be noted, however, that in modern Italian doctrine (e.g., Magliulo, *La Fusione Delle Società*) and judicial decisions (*Cass. civ. SS.UU. 2637/2006*, 129 Il Foro Italiano) a merger does not entail any transfer between companies, but is merely a modification of the statute. The *Garante* correctly notes this perspective, and bases its decision not on an analogy with the transfer to third countries but on the principle of fair processing.

[279] In re Doubleclick Inc. Privacy Litigation, 154 F. Supp.2d.

[280] For more detail see: Schwabach, *Internet and the Law*, 97.

[281] European Commission, *Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover*.

[282] Verwaltungsgericht Hamburg, *24.04.2017 - 13 E 5912/16*.

[283] The position in the text is the one expressed in European Data Protection Supervisor, "EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data." The EDPS suggests that the Commission should consider personal data as a parameter to assess whether a merger should be subject to investigation.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

potential solutions. The size of this problem is such that it has led to a parallel form of business, called cloud brokering, whose objective is to guide the potential enterprise in the choice of a cloud service provider, untwining the tangle of differential features.

As the cloud marketplace expands and matures, legal issues that may arise from the use of cloud computing are gaining prominence. Cloud services operate under a multitude of interwoven regimes, which sometimes do not perfectly fit with each other. The legal concept of property is jeopardized when seen in the context of cloud computing, and not from a merely theoretical point of view. The two perspectives of property *of* the cloud and property *in* the cloud display very peculiar features, and require different forms of protection. Information placed in the cloud coexists with the hardware and software assets making up the cloud itself, and it is placed under the control of the cloud provider. Therefore it is important that the rights over the content in the cloud be kept well distinct from the rights over the cloud assets. By doing so, it is possible for the cloud customer to avoid undesired consequences such as the loss of IPRs to the cloud provider, or information having an economic value falling into the bankrupt estate in case the cloud provider files for bankruptcy. Conversely, the cloud provider's intellectual properties need to be protected horizontally from unfair business practices by competitors, and vertically from possible illicit behaviors by customers. As a huge number of individuals and businesses use the cloud to store their data or to provide their services, the economic impact of such issues is potentially enormous.

Unfortunately, the existing legal framework is generally anchored to older business models. This is not a problem *per se*, as cloud services must be subject to the same business rules as any other undertaking. However, the peculiarities of cloud computing require an attentive analysis of the various legal domains that affect that business, and especially of the interactions between the various regimes. Although courts have not given a lot of attention to cloud computing yet, doctrine and institutions, including the European Commission, are striving to shape the context in which it operates. Most relationships relating to cloud services will have a contractual base: customers agree to the terms and conditions with the cloud service provider, and also the service providers shall contract with each other for the supply of their services. This contractual interlacing resides mostly on the commercial decisions of the involved players, rather than being drafted among the parties in a customizable fashion. Even if the existing European laws give some answers about the data which is created and brought to the cloud by the players, ambiguity yet resides for the allocation of property rights of the data produced in the cloud, such as derived information or liability for the content. The law of contract can play an important role as private governance, on the allocation of information ownership in what refers mostly on confidentiality, and copyright.

In a *de iure condendo* perspective, a uniform legislative approach would be advisable. Internet services should not be considered like traditional enterprises. They operate in a global market, being available to anybody worldwide. Consequently, the legal regime in which they operate will frequently not be the same as that of their customers. A unified approach, such as one based on international legislation (e.g., a WIPO treaty), would provide benefits to cloud customers (both businesses and individuals), by establishing uniform terms and conditions which drive consistency in the protection of IPRs and data in the cloud.

REFERENCES

Abdel Wahab MS, Katsh ME, Rainey D, editors. Online dispute resolution: theory and practice: a treatise on technology and dispute resolution. The Hague: Portland, OR: Eleven International Publishing; 2012.

Abrams M. The origins of personal data and its implications for governance. SSRN Electron J 2014;https://doi.org/10.2139/ssrn.2510927.

Adriasola Navarrete, José Manuel. *La Transformación de La Empresa*. Editorial Jurídica de Chile, 1971.

Al-Khouri AM. Data ownership: who owns 'my data'? Int J Manag Inf Technol 2007;2(1):1–8.

Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, et al. A view of cloud computing. Commun ACM 2010;53(4):50–8.

Article 29 Data Protection Working Party. Opinion 7/2003 on the Re-Use of Public Sector Information and the Protection of Personal Data: Striking the Balance," 2003. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf. [Accessed 27 November 2017].

Article 29 Data Protection Working Party. Article 29 Data Protection Working Party. Opinion 1/2010 on the Concepts of 'Controller' and 'Processor', 2010. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf. [Accessed 27 November 2017].

Article 29 Data Protection Working Party. Opinion 15/2011 on the Definition of Consent," 2011. Available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf. [Accessed 27 November 2017].

Article 29 Data Protection Working Party. Opinion 03/2013 on Purpose Limitation," 2013. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. [Accessed 27 November 2017].

Article 29 Data Protection Working Party. Opinion 06/2013 on Open Data and Public Sector Information ('PSI') Reuse," 2013. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf. [Accessed 27 November 2017].

Azeez A, Perera S, Gamage D, Linton R, Siriwardana P, Leelaratne D, et al. "Multi-Tenant SOA Middleware for Cloud Computing." In Proceedings of the 3Rd International Conference on Cloud Computing (CLOUD), 458–465. IEEE, 2010.

Barham P, Dragovic B, Fraser K, Hand S, Harris T, Ho A, et al. "Xen and the Art of Virtualization," 164. ACM Press, 2003. https://doi.org/10.1145/945445.945462.

Bartolini C, El Kateb D, Le Traon Y, Hagen D. Cloud providers viability: how to address it from an IT and legal perspective? In: Altmann J, Silaghi GC, Rana OF, editors. Economics of Grids, Clouds, Systems, and Services, vol. 9512. Computer Communication Networks and Telecommunications. Springer International Publishing; 2016. p. 281–95.

Bennett K, Layzell P, Budgen D, Brereton P, Macaulay L, Munro M. Service-Based Software: The Future for Flexible Software." In Proceedings of the 7Th Asia-Pacific Software Engineering Conference (APSEC), 214–221. IEEE, 2000.

Berle AA Jr. The theory of enterprise entity. Columbia Law Rev 1947;47(3):343–58.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

Bessen J, Hunt RM. An empirical look at software patents. J Econ Manag Strategy 2007;16(1):https://doi.org/10.1111/j.1530-9134.2007.00136.x.

Bezemer C-P, Zaidman A. Multi-Tenant SaaS applications: maintenance dream or nightmare? In: 2010 In Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), 88–92. ACM.

BGH: Shift.Tv, Urteil v. 22.04.2009, Az. I ZR 216/06." Gewerblicher Rechtsschutz Und Urheberrecht (GRUR), 2009, 845–852.

Bianca CM. *La Proprietà*. Vol. VI. Diritto Civile. Giuffré, 1999.

Bradley-Schmieg P, Jones J. *CJEU Confirms That National Data Retention Laws May Only Be Adopted Where "Strictly Necessary"*, 2017. Available from: https://www.insideprivacy.com/international/european-union/cjeu-confirms-that-national-data-retention-laws-may-only-be-adopted-where-strictly-necessary/. [Accessed 27 November 2017].

Bradshaw S, Millard C, Walden I. Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services. Int J Law Inf Technol 2011;19(3):187–223.

Bretan J. Harboring doubts about the efficacy of § 512 immunity under the DMCA. Annu Rev Law Technol 2003;18(1):43–67.

Bundesgerichtshof (Zivilsachen). *Urt. v. 07.06.1990*, Az.: III ZR 74/88: Puffreisriegel, 1990. Available from: https://www.jurion.de/Urteile/BGH/1990-06-07/III-ZR-74_88. [Accessed 27 November 2017].

Buttarelli G. *The Impact of the General Data Protection Regulation on Collaborative Science in Europe and the European Cloud Initiative*. Brussels, 2016. Available from: https://edps.europa.eu/sites/edp/files/publication/16-10-18_speech_isc_en.pdf. [Accessed 27 November 2017].

California Northern District Court. In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A, Document 45, No. 3:2016mc80263 (California Northern District Court). 2016.

Callamard A. Are Courts Re-Inventing Internet Regulation? Int Rev Law Comput Technol 2017;31(3):323–39. https://doi.org/10.1080/13600869.2017.1304603.

Calloway TA. Cloud computing, clickwrap agreements, and limitation on liability clauses: a perfect storm. Duke Law Technol Rev 2012;11(1):163–74.

Casalicchio E, Palmirani M. A cloud service broker with legal-rule compliance checking and quality assurance capabilities. Procedia Comput Sci 2015;68:136–50. https://doi.org/10.1016/j.procs.2015.09.230.

Cheung ASY, Weber RH. editors. Privacy and legal issues in cloud computing. In: Elgar law, technology and society. Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing; 2015.

Christie A. Designing appropriate protection for computer programs. Eur Intellect Prop Rev 1994;16(11):486–93.

Coco Cloud. First Study of Legal and Regulatory Aspects of Cloud Computing." Project deliverable. Coco Cloud - Confidential and Compliant Clouds, Project co-funded by the European Commission within the Seventh Framework Programme, FP7-ICT-2013-10 Coco Cloud - GA#610853, 2014.

Colombo GE. *Il Trasferimemto [Sic] Dell'azienda e Il Passaggio Dei Crediti e Dei Debiti*. Padova: CEDAM, 1972.

Commission Nationale de l'Informatique et des Libertés (CNIL). *Right to Be Delisted: The CNIL Restricted Committee Imposes a €100,000 Fine on Google*, 2016. Available from: https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google. [Accessed 27 November 2017].

Committee on Industry, Research and Energy, and Committee on the Internal Market and Consumer Protection. *Report on Towards a Digital Single Market Act*, 2015. Available from: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2015-0371&format=XML&language=EN. [Accessed 27 November 2017].

Computer Associates International, Inc. v. *Altai, Inc.*, 982 F.2d 693 (2d Cir.). 1992.

Connor I. Database Rights Are No 'Impediment' to Europe's Data-Driven Economy: A Legal Expert Explains How Robust Rights Support Innovation," 2016. Available from: https://www.theregister.co.uk/2016/01/14/database_rights_are_no_impediment_to_the_growth_of_europes_datadriven_economy_expert_says/. [Accessed 27 November 2017].

Corrales M, Djemame K. "A brokering framework for assessing legal risks in big data and the cloud. In: Corrales M, Fenwick M, Forgó N, editors. New technology, big data and the law. Singapore: Springer Singapore; 2017. p. 187–222 https://doi.org/10.1007/978-981-10-5038-1_8.

Corte di Cassazione. Sentenza 11 agosto 1990, n. 8219 (Corte di Cassazione August 11, 1990).

Corte di Cassazione, Sezioni Unite civili. Ordinanza 8 febbraio 2006, n. 2637, 129 Il Foro Italiano 1739 (Corte di Cassazione, Sezioni Unite civili 2006).

Court of Justice of the European Union. *Freistaat Bayern* v *Verlag Esterbauer GmbH*: C-490/14, ECLI:EU:C:2015:735, 2014.

de Matos J, Varela A, de Lima P. Código Civil Anotado, vol. I. 4th ed. Coimbra editora; 2010.

Daskal J. Law enforcement access to data across borders: the evolving security and rights issues. J National Secur Law Policy 2016;8(3):473–501.

De Filippi P. Law of the cloud: on the supremacy of the user interface over copyright law. Internet Policy Rev 2013;2(3):https://doi.org/10.14763/2013.3.175.

De Filippi P, McCarthy S. Cloud computing: centralization and data sovereignty. Eur J Law Technol 2012;3(2):http://ejlt.org/article/view/101.

De Sola Pool I, Solomon RJ. Intellectual property and transborder data flows. Stanford J Int Law 1980;16:113–39.

Debeauvais T, Nardi B. A Qualitative Study of Ragnarök Online Private Servers: In-Game Sociological Issues." In Proceedings of the 5Th International Conference on the Foundations of Digital Games (FDG), 48–55. ACM, 2010.

Derclaye E. Databases Sui Generis right: should we adopt the spin-off theory? Eur Intellect Prop Rev 2004;26(9):402–13.

Di Martino B, Cretella G, Esposito A. Towards a legislation-aware cloud computing framework. Procedia Comput Sci 2015;68:127–35. https://doi.org/10.1016/j.procs.2015.09.229.

Dinh HT, Lee C, Niyato D, Wang P. A survey of mobile cloud computing: architecture, applications, and approaches: a survey of mobile cloud computing. Wireless Commun Mobile Comput 2013;13(18):1587–611. https://doi.org/10.1002/wcm.1203.

Diver L. Would the current ambiguities within the legal protection of software be solved by the creation of a sui generis property right for computer programs? J Intellect Prop Law Pract 2008;3(2):125–38. https://doi.org/10.1093/jiplp/jpm228.

Djemame K, Barnitzke B, Corrales M, Kiran M, Jiang M, Armstrong D, et al. Legal issues in clouds: towards a risk inventory. Philos Trans A Math Phys Eng Sci 2012;371(1983): https://doi.org/10.1098/rsta.2012.0075. 20120075–20120075.

von der Dunk FG. A European 'Equivalent' to United States Export Controls: European Law on the control of international trade in dual-use space technologies. Astropolitics 2009;7(2):101–34. https://doi.org/10.1080/14777620903094826.

Dusollier S. Electrifying the fence: the legal protection of technological measures for protecting copyright. Eur Intellect Prop Rev 1999;21(6):285–97.

Ehrlich P. Communications Decency Act § 230. Annu Rev Law Technol 2002;17(1):401–19.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

Eisner RS, Oram MA. Clear skies or stormy weather for cloud computing? Critical privacy and security contracting issues for customers of cloud computing. In: Sotto LJ, Smedinghoff TJ, Kennedy JB, Gilbert F, editors. Privacy and data security law institute (Eleventh Annual). Intellectual Property Course Handbook G1005, G1006. 2010 Practising Law Institute.
Epping V. Die Aussenwirtschaftsfreiheit. Tübingen: Mohr Siebeck; 1998.
European Commission, "Communication from the Commission: Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings." 2009a.
European Commission, "Legal Analysis of a Single Market for an Information Society: Liability of Online Intermediaries." 2009b. Available from: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=835. [Accessed 27 November 2017].
European Commission. *Antitrust: Statement on Apple's IPhone Policy Changes*, 2010. Available from: http://europa.eu/rapid/press-release_IP-10-1175_en.htm. [Accessed 27 November 2017].
European Commission,"Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe." 2012.
European Commission. Report of the European Commission Conference of 29 June 2012 "Trade Secrets: Supporting Innovation, Protecting Know-How," 2012. Available from: http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8270. [Accessed 27 November 2017].
European Commission, "European Commission - Fact Sheet: Questions and Answers - Data Protection Reform." 2015a. Available from: http://europa.eu/rapid/press-release_MEMO-15-6385_it.htm. [Accessed 27 November 2017].
European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe." 2015b.
European Commission,"Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Modern, More European Copyright Framework." 2015c.
European Commission. Antitrust: Commission Sends Statement of Objections to Google on Android Operating System and Applications: Factsheet. European Commission, 2016.
European Commission. *Cloud Security Workshop: Building Trust in Cloud Services - Certification and Beyond*. Brussels, Belgium: European Commission, 2016. Available from: https://ec.europa.eu/digital-single-market/en/news/cloud-security-workshop-building-trust-cloud-services-certification-and-beyond. [Accessed 27 November 2017].
European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Cloud Initiative - Building a Competitive Data and Knowledge Economy in Europe." 2016. Available from: https://ec.europa.eu/digital-single-market/en/news/communication-european-cloud-initiative-building-competitive-data-and-knowledge-economy-europe. [Accessed 27 November 2017].
European Commission. *Results of the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries, Data and Cloud Computing and the Collaborative Economy*, 2016. Available from: https://ec.europa.eu/digital-single-market/en/news/results-public-consultation-regulatory-environment-platforms-online-intermediaries-data-and. [Accessed 27 November 2017].
European Commission. *Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover*, 2017. Available from: http://europa.eu/rapid/press-release_IP-17-1369_en.htm. [Accessed 27 November 2017].
European Copyright Society. General Opinion on the EU Copyright Reform Package," 2017. Available from: https://europeancopyrightsocietydotorg.files.wordpress.com/2015/12/ecs-opinion-on-eu-copyright-reform-def.pdf. [Accessed 27 November 2017].
European Copyright Society. *General Opinion on the EU Copyright Reform Package*, 2017. Available from: https://europeancopyrightsociety.org/2017/01/25/opinion-on-eu-reform-package/. [Accessed 27 November 2017].
European Data Protection Supervisor. "EDPS Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data," 2016. https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf. [Accessed 27 November 2017].
European Patent Office. *T 0208/84 (Computer-Related Invention) of 15.7.1986: ECLI:EP:BA:1986:T020884.19860715*, 1986.
European Patent Office. *T 1173/97 (Computer Program Product/IBM) of 1.7.1998: ECLI:EP:BA:1998:T117397.19980701*, 1998.
Evans BJ. Much ado about data ownership. Harv J Law Technol 2011;25(1):69–130.
Expert Group on Cloud Computing Contracts. *Unfair Contract Terms in Cloud Computing Service Contracts Discussion Paper*, 2014. Available from: http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_unfair_contract_terms_en.pdf. [Accessed 27 November 2017].
Fairén Guillén V, Gomez Colomer JL. *Estudios Sobre La Ley de Enjuiciamiento Civil y Su Práctica Inicial*. Dykinson, 2004.
Fenno E, Humphries C. Commun Lawyer 2011;28(2):28–37. 1.
Ferrara F, Corsi F. *Gli Imprenditori e Le Società*. XV. Giuffré, 2011.
Foss K. *Will Software Piracy Fears Keep Adobe Products out of China?*, 2002. Available from: http://www.planetpdf.com/mainpage.asp?webpageid=1891. [Accessed 27 November 2017].
Founds GL. Shrinkwrap and Clickwrap Agreements: 2B or not 2B? Fed Commun Law J 1999;52(1):99–123.
Frosio GF. Reforming intermediary liability in the platform economy: a European digital single market strategy. Northwest Univ Law Rev Online 2017;111.
Garante per la protezione dei dati personali. *Provisions Applying to Corporate Mergers and Split-Ups*, 2009. Available from: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1625292. [Accessed 27 November 2017].
Garrote Fernández-Díez I. Comparative Analysis on National Approaches to the Liability of Internet Intermediaries for Infringement of Copyright and Related Rights." World Intellectual Property Organization (WIPO), 2014. Available from: http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries_garrote.pdf. [Accessed 27 November 2017].
Garrouste P The new property rights theory of the firm. In: Colombatto E., editor. The Elgar Companion to the economics of property rights. Edward Elgar Publishing Limited; n.d. p. 370–82.
Garrouste P, Saussier S. Looking for a theory of the firm: future challenges. J Econ Behav Organ 2005;58(2):178–99.
Gatt A. Electronic commerce – click-wrap agreements: the enforceability of click-wrap agreements. Comput Law Secur Rev 2002;18(6):404–10. https://doi.org/10.1016/S0267-3649(02)01105-6.
Géczy P, Izumi N, Hasida K. Cloudsourcing: managing cloud adoption. Glob J Bus Res 2012;6(2):57–70.
Ginsburg JC, Treppoz E. International copyright law. Edward Elga Publishing; 2015.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

Givon M, Mahajan V, Muller E. Software piracy: estimation of lost sales and the impact on software diffusion. J Mark 1995;59(1):29–37.

Google, Inc. and Onix Networking Corporation v. *The United States and Softchoice Corporation* (United States Court of Federal Claims). 2011.

Google Spain SL and Google Inc. v *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*: C-131/12, ECLI:EU:C:2014:317, 2014.

Graham SJH, Mowery DC. Cohen WM, Merrill SA, editors. Intellectual property protection in the U.S. software industry. The National Academies Press; 2003. p. 219–58 https://doi.org/10.17226/10770.

Grossman RL, Greenway M, Heath AP, Powell R, Suarez RD, Wells W, et al. The Design of a community science cloud: the open science data cloud perspective. IEEE 2012;1051–7. https://doi.org/10.1109/SC.Companion.2012.127.

Grossman SJ, Hart OD. The costs and benefits of ownership: a theory of vertical and lateral integration. J Polit Econ 1986;94(4):691–719.

Group on Earth Observations. *White Paper: Mechanisms to Share Data as Part of GEOSS Data-CORE*. Group on Earth Observations, 2014. Available from: https://www.earthobservations.org/documents/dswg/Annex%20VI%20-%20%20Mechanisms%20to%20share%20data%20as%20part%20of%20GEOSS%20Data_CORE.pdf.

Guild E, Carrera S. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive." CEPS Liberty and Security in Europe Papers. Centre for European Policy Studies, 2014.

Hart O, Moore J. Property rights and the nature of the firm. J Polit Econ 1990;98(6):1119–58.

Helmbrecht U. Data protection and legal compliance in cloud computing. Datenschutz Und Datensicherheit - DuD 2010;34(8):554–6. https://doi.org/10.1007/s11623-010-0189-x.

Hildebrandt M, Gutwirth S, editors. Profiling the European citizen: cross-disciplinary perspectives. New York: Springer; 2008.

Hinduja S. Correlates of internet software piracy. J Contemp Crim Justice 2001;17(4):369–82. https://doi.org/10.1177/1043986201017004006.

Hoffa C, Mehta G, Freeman T, Deelman E, Keahey K, Berriman B, et al. On the use of cloud computing for scientific workflows. IEEE 2008;640–5. https://doi.org/10.1109/eScience.2008.167.

Hon WK, Millard C, Walden I. Who is responsible for 'Personal Data' in cloud computing?—the cloud of unknowing, Part 2. Int Data Priv Law 2012;2(1):3–18. https://doi.org/10.1093/idpl/ipr025.

Hughes J. The philosophy of intellectual property. Geo L J 1988;77(2):287–366.

Information Commissioner's Office. Big Data, Artificial Intelligence, Machine Learning and Data Protection." Information Commissioner's Office, 2017.

IMS Health GmbH & Co. OHG v *NDC Health GmbH & Co. KG.*: C-418/01, ECLI:EU:C:2004:257, 2004.

International Organization for Standardization. ISO 27018: Information Technology – Security Techniques – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors." Standard. International, 2014.

Jacobs A. The pathologies of big data. Commun ACM 2009;52(8):36. https://doi.org/10.1145/1536616.1536632.

Johannsen K. § 89 Versicherung Für Inbegriff von Sachen." In §§ 74–99 VVG, edited by Horst Baumann, Roland Michael Beckmann, Katharina Johannsen, and Ralf Johannsen, 9th ed., 3:613–621. Großkommentare Der Praxis. De Gruyter, 2009.

Kafeza I, Kafeza E, Panas E. Contracts in Cloud Computing." In Proceedings of the 2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 1–8, 2014.

Kaisler S, Armour F, Espinosa JA, Money W. Big data: issues and challenges moving forward. IEEE 2013;995–1004. https://doi.org/10.1109/HICSS.2013.645.

Katsh ME, Rifkin J. Online dispute resolution: resolving conflicts in cyberspace. 1st ed. San Francisco: Jossey-Bass; 2001.

Katz A. A network effects perspective on software piracy. Univ Tor Law J 2005;55(2):155–216.

Keller D. The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation," 2017. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684. [Accessed 27 November 2017].

Kerr IR, Maurushat A, Tacit CS. Technical protection measures: tilting at Copyright's Windmill. Ottawa Law Rev 2002;34(2):7–82.

Krebs R, Momm C, Kounev S. Architectural Concerns in Multi-Tenant SaaS Applications." In Proceedings of the 2nd International Conference on Cloud Computing and Services Science (CLOSER), edited by Frank Leymann, Ivan Ivanov, Marten van Sinderen, and Tony Shan, 426–431. SciTePress, 2012. https://doi.org/10.5220/0003957604260431.

Kwok T, Mohindra A. Resource Calculations with Constraints, and Placement of Tenants and Instances for Multi-Tenant SaaS Applications." In Proceedings of the 6Th Service-Oriented Computing - ICSOC 2008, edited by Athman Bouguettaya, Ingolf Krueger, and Tiziana Margaria, 5364:633–648. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2008.

Kin Wai Lau Eric. An empirical study of software piracy. Bus Ethics 2003;12(3):233–45.

Layne-Farrar A. Defining software patents: a research field guide. SSRN Electron J, 2006. https://doi.org/10.2139/ssrn.1818025.

Lee D, Fulford T. Virtual empires. Cult Critique 2000;(44):3. https://doi.org/10.2307/1354600.

Lehmann R. *How Much Will Google Reader's Demise Cost Your Business?*, 2013. Available from: https://moz.com/ugc/how-much-will-google-readers-demise-cost-your-business. [Accessed 27 November 2017].

Leifeld P, Haunss S. Political discourse networks and the conflict over software patents in europe: political discourse networks. Eur J Polit Res 2012;51(3):382–409. https://doi.org/10.1111/j.1475-6765.2011.02003.x.

Lemley MA. Convergence in the law of software copyright. Berkeley Technol Law J 1995;10(1):1–34. https://doi.org/10.15779/Z38CQ2M.

L'Oréal SA and Others v *eBay International AG and Others*: C-324/09, ECLI:EU:C:2011:474, 2011.

Macías M, Guitart J. Client classification policies for SLA negotiation and allocation in shared cloud datacenters. In: Vanmechelen K, Altmann J, Rana OF, editors. Economics of Grids, Clouds, Systems, and Services. 7150. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. p. 90–104 https://doi.org/10.1007/978-3-642-28675-9_7.

MacQueen HL, Waelde C, Laurie G, Brown A, Contemporary intellectual property: law and policy. 2nd ed. Oxford: Oxford Univ. Press; 2010.

Magliulo F. *La Fusione Delle Società*. Second. Notariato e Nuovo Diritto Societario 5. IPSOA, 2009.

Marks DS, Turnbull BH. Technical protection measures: the intersection of technology, law and commercial licenses. J Copyr Soc USA 1999;46(4):563–601.

Marlow S, Spuhl U, Schneider C, Schirmer H, Goergen E-M, Marko V, et al. *Das Neue VVG Kompakt: Ein Handbuch Für Die Rechtspraxis*. 4th ed. Verlag Versicherungswirtschaft, 2010.

Martic D. Online Dispute Resolution for Cloud Computing Services. In Proceedings of the First JURIX Doctoral

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

Consortium and Poster Sessions in Conjunction with the 26th International Conference on Legal Knowledge and Information Systems (DoCoPe@JURIX), 2013.
Martic D. Redress for Free Internet Services under the Scope of the EU and UNCITRAL's ODR Regulations." Democracia Digital e Governo Eletrônico 1, no. 10 (2014): 360–76.
Martic D. Dispute Resolution for Cloud Services: Access to Justice and Fairness in Cloud-Based Low-Value Online Services." PhD thesis, Università di Bologna, 2017.
Mattel, Inc. v. *MGA Entertainment, Inc.*, 616 F.3d 904 (9th Cir.). 2010.
Mayer FC. Europe and the internet: the old world and the new medium. Eur J Int Law 2000;11(1):149–69.
Mell PM, Grance T. The NIST Definition of Cloud Computing." Gaithersburg, MD: National Institute of Standards and Technology, 2011. https://doi.org/10.6028/NIST.SP.800-145.
Menell PS. An analysis of the scope of copyright protection for application programs. Stanford Law Rev 1989;41(5):1045–104. https://doi.org/10.2307/1228751.
Meurer MJ. Price discrimination, personal use and piracy: copyright protection of digital works. Buffalo Law Rev 1997;45:846–90. https://doi.org/10.2139/ssrn.49097.
Microsoft Corp. v. *United States*, 829 F.3d 197 (2d Cir.). 2016.
Moore J. The firm as a collection of assets. Eur Econ Rev 1992;36(2–3):493–507.
Möller H, Sieg K. Kommentar Zum Versicherungsvertragsgesetz Und Allgemeine Versicherungsbedingungen Unter Einschluß Des Versicherungsvermittlerrechts, vol. 2. 8th ed. De Gruyter; 1980.
Muchmore M. *Stolen Software: Piracy Hits More than Movies and Music*, 2012. Available from: http://www.pcmag.com/article2/0,2817,2399315,00.asp. [Accessed 27 November 2017].
Muir I, Brandi-Dohrn M, Gruber S. European patent law: law and procedure under the EPC and PCT. 2nd ed. Oxford: Oxford Univ. Press; 2002.
Naumov V, Amosova A. Providers' liability. AmCham News 2010;16(88):26–8.
Naylor D, Ritter C. French judgment condemning AOL illustrates EU consumer protection issues facing U.S. businesses operating in Europe. New York Univ J Law Bus 2005;1(3):881–97.
Noble Foster T. Navigating through the fog of cloud computing contracts. John Marshall J Inf Technol Priv 2013;30(1):13–30.
Norwegian Consumer Council, "Hazy Terms in the Cloud: A Short Study of the Terms and Conditions of Cloud Storage Services." 2014. Available from: https://fil.forbrukerradet.no/wp-content/uploads/2014/02/2014-05-14-Unfair-cloud-storage-terms_report.pdf. [Accessed 27 November 2017].
Oscar E, Ochoa G. *Bienes y Derechos Reales*. Vol. II. Derecho Civil. Universidad Católica Andres Bello, 2008.
Ohm P. Broken promises of privacy: responding to the surprising failure of anonymization. UCLA Law Rev 2010;57(6):1701–77.
Ojala A. Software-as-a-Service revenue models. IT Prof 2013;15(3):54–9. https://doi.org/10.1109/MITP.2012.73.
Padhy RP, Patra MR, Satapathy SC. SLAs in cloud systems: the business perspective. Int J Comput Sci Technol 2012;3(1):481–8.
Parrilli DM. Software patentability in a grid environment. SSRN Electron J 2008;https://doi.org/10.2139/ssrn.1275227.
Parrilli DM. Grid and Cloud Computing as a Tool to Transform European Economy: Legal Considerations." In Proceedings of the 48th FITCE Congress, 138–41. Prague: FITCE, 2009.
Petersen C, DeMuro P. Legal and regulatory considerations associated with use of patient-generated health data from social media and mobile health (MHealth) devices. Appl Clin Inform 2015;6(1):16–26. https://doi.org/10.4338/ACI-2014-09-R-0082.
Pila J. Software patents, separation of powers, and failed syllogisms: a cornucopia from the enlarged Board of Appeal of the European Patent Office. Camb Law J 2011;70(01):203–28. https://doi.org/10.1017/S0008197311000225.
Pistorius T. Shrink-wrap and click-wrap agreements. Juta's Bus Law 1999;7(3):79–86.
Prime Minister of Japan and His Cabinet, "Intellectual Property Strategy Headquarters." 2016. Available from: http://japan.kantei.go.jp/97_abe/actions/201605/09article3.html. [Accessed 27 November 2017].
Radin MJ. Information tangibility. SSRN Electron J 2002;https://doi.org/10.2139/ssrn.357060.
Rappa MA. The utility business model and the future of computing services. IBM Syst J 2004;43(1):32–42.
Rashbaum KN, Borden BB, Beaumont TH. Outrun the lions: a practical framework for analysis of legal issues in the evolution of cloud computing. Ave Maria Law Rev 2014;12(1):71–102.
Reed C. Information 'Ownership' in the Cloud. Research Paper. Queen Mary University of London, School of Law, 2010. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461##. [Accessed 27 November 2017].
Reed C. Information in the cloud: ownership, control and accountability. In: Cheung A, Weber R, editors. Privacy and legal issues in cloud computing. Edward Elgar Publishing; 2015. p. 139–59 https://doi.org/10.4337/9781783477074.00014.
Rojina Villegas R. *Bienes, Derechos Reales y Sucesiones*. 41st ed. Vol. II. Compendio de Derecho Civil, 2008.
Rowland D, Kohl U, Charlesworth A. Information technology law. 4th ed. Abingdon, Oxon; New York: Routledge; 2012.
Rule C. Online dispute resolution for business: B2B, e-Commerce, Consumer, Employment, Insurance, and Other Commercial Conflicts. 1st ed. San Francisco: Jossey-Bass; 2002.
Samuelson P. CONTU revisited: the case against copyright protection for computer programs in machine-readable form. Duke Law J 1984;33(4):663–769.
Satanowsky M. Nature juridique de l'entreprise et du fonds de commerce. Rev Int Droit Comparé 1955;7(4):726–50. https://doi.org/10.3406/ridc.1955.9987.
Schaffer HE. X as a service, cloud computing, and the need for good judgment" 11, 5 (2009): 4–5.
Schwabach A. Internet and the Law: technology, society, and compromises. 2nd ed. Santa Barbara, Calif.: ABC-CLIO; 2014.
Senftleben M. Breathing space for cloud-based business models. JIPITEC - J Intellect Prop Inf Technol E-Commerce Law 2013;4(2):87–103.
Seng D. Comparative Analysis of the National Approaches to the Liability of Internet Intermediaries." World Intellectual Property Organization (WIPO), 2010. Available from: http://www.wipo.int/export/sites/www/copyright/en/doc/liability_of_internet_intermediaries.pdf. [Accessed 27 November 2017].
Silva Segura E. *Acciones, Actos y Contratos Sobre Cuota: El Problema Jurídico y Práctico de Las Acciones y Derechos*. Editorial Samver, 1970.
Soat J. *Why Cloud Databases Are In Your Future*, 2015. Available from: https://www.forbes.com/sites/oracle/2015/01/28/why-cloud-databases-are-in-your-future/#7d864a2e5aed. [Accessed 27 November 2017].
Software & Information Industry Association. *Software as a Service: Strategic Backgrounder*, 2001. Available from: http://www.slideshare.net/Shelly38/software-as-a-service-strategic-backgrounder. [Accessed 27 November 2017].
Solove DJ, Schwarz PM. *Information Privacy Law*. 3rd Wolters Kluwer Law & Business, 2009.
Sotto LJ, Treacy BC, McLellan ML. Privacy and data security risks in cloud computing. World Commun Regul Rep 2010;5(2).
Staatssecretaris van Financiën v *X BV*: C-651/11, ECLI:EU:C:2013:346, 2011.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005

Steier R. Legally speaking. Commun ACM 1989;32(12):1391. https://doi.org/10.1145/76380.316016.
Stern RH. Another look at copyright protection of software: did the 1980 act do anything for object code? John Marshall J Inf Technol Priv Law 1981;3(1):1–17.
Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 2011;34(1):1–11.
Supreme Court of Canada. *Google Inc.* v. *Equustek Solutions Inc.*, Case 36602, 2017.
Supreme Court of Louisiana. *In Re: Howard Marshall Charitable Remainder Annuity Trust*, 1998.
Swire PP, Lagos Y. Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique. SSRN Electron J 2013;https://doi.org/10.2139/ssrn.2159157.
Tele2 Sverige AB v *Post- Och Telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*: Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, 2016.
TETS Haskovo AD v *Direktor Na Direktsia "Obzhalvane i Upravlenie Na Izpalnenieto"*: C-234/11, ECLI:EU:C:2012:644, 2011.
The European Consumer Organisation. *Putting an End to Silos in the Enforcement of Consumers' Rights*, 2016. Available from: http://www.beuc.eu/publications/putting-end-silos-enforcement-consumers%E2%80%99-rights/html. [Accessed 27 November 2017].
The Trademark Company. *Brand Protection for Cloud Computing*. The Trademark Company, 2014. Available from: http://www.thetrademarkcompany.com/learning-center/brand-protection-for-cloud-computing. [Accessed 27 November 2017].
Timofeeva YA. Hate speech online: restricted or protected – comparison of regulations in the United States and Germany. J Transnat'l L Pol'y 2003;12(2):253–86.
Valcke P, Kuczerawy A, Ombelet P-J. Did the Romans get it right? What Delfi, Google, eBay, and UPC TeleKabel Wien have in common. In: Taddeo M, Floridi L, editors. The responsibilities of online service providers. 31. Cham: Springer International Publishing; 2017. p. 101–16 https://doi.org/10.1007/978-3-319-47852-4_6.
Vaquero LM, Rodero-Merino L, Caceres J, Lindner M. A break in the clouds: towards a cloud definition. ACM SIGCOMM Comput Commun Rev 2009;39(1):50–5.
Verbiest T, Spindler G, Riccio GM, Van der Perre A. Study on the Liability of Internet Intermediaries. European Commission 2007;Available from: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf. [Accessed 27 November 2017].
Verwaltungsgericht Hamburg. *Beschluss: 24.04.2017 - 13 E 5912/16*, 2017.
Victor JM. The EU general data protection regulation: toward a property regime for protecting data privacy. Yale Law J 2013;123(2):513–28.
Visser D. The database right and the spin-off theory. In: Snijders HJ, Weatherill S, editors. E-Commerce Law. The Hague/London/New York: Kluwer Law International; 2003. p. 105–10.
Walden I, Luciano LDC. Ensuring competition in the clouds: the role of competition law? SSRN Electron J 2011;https://doi.org/10.2139/ssrn.1840547.
Wang L, von Laszewski G, Younge A, He X, Kunze M, Tao J, et al. Cloud computing: a perspective study. New Generation Comput 2010;28(2):137–46.
Weber RH. The digital future – a challenge for privacy? Comput Law Secur Rev 2015;31(2):234–42. https://doi.org/10.1016/j.clsr.2015.01.003.
Weckström K. Trademarks in new markets: simple infringement or cause for evaluation? J Int Commer Law Technol 2012;7(4):300–17.
Whelan Associates Inc. v. *Jaslow Dental Laboratory, Inc.*, 797 F.2d 1222 (3d Cir. 1986).
Wieling HJ. Sachenrecht. In: Enzyklopädie Der Rechts- Und Staatswissenschaft, vol. 1. 2nd ed. Springer Berlin Heidelberg. 2006.
Yiannopoulos AN. Introduction to the law of things: Louisiana and Comparative Law. LA Law Rev 1962;22(4):756–97.
Your Response Ltd v *Datateam Business Media Ltd* (England and Wales Court of Appeal 2014).
Zarsky TZ. 'Mine Your Own Business!': making the case for the implications of the data mining of personal information in the forum of public opinion. Yale J Law Technol 2003;5(1):1–56.

Please cite this article in press as: Cesare Bartolini, Cristiana Santos, Carsten Ullrich, Property and the cloud, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.10.005