***IBIMA Publishing***
*Journal of Cloud Computing*
*http://www.ibimapublishing.com/journals/JCC/jcc.html*
*Vol. 2014 (2014), Article ID 683295, 12 pages*
*DOI: 10.5171/2014.683295*

*Research Article*

# Cloud Cover: Protecting Innovations

**Susan Keston**

Harrison Goddard Foote LLP, Delta House, Glasgow, United Kingdom

skeston@hgf.com

Received date: 14 November 2013; Accepted date: 27 January 2014;
Published date: 13 August 2014

**Abstract**

There are special considerations for intellectual property when considered in the context of cloud computing. Innovations in the technological field of cloud computing are considered, with a focus on the availability of patent protection. A claim drafting strategy is devised taking account of the characteristic features of cloud based architectures and considering enforceability of the claims upon grant of the patent. The use of cloud technology to facilitate innovation in technological fields other than cloud computing is also considered with a focus on safeguarding absolute novelty, which is a prerequisite for patent protection. Open source software and software licences are also discussed from the perspective of the cloud.

**Keywords:** intellectual property, patents, software licences, cloud computing

## Introduction

Cloud computing is a rapidly growing technology area, which is a fertile ground for innovation and has the potential to revolutionise the field of information technology. Cloud computing systems tend to be complex due to their dynamic architecture and are typically deployed across multiple legal jurisdictions. Although this presents challenges in protecting cloud based inventions due to the nature of patents, which are territorial rights, these challenges can be met given a carefully thought out intellectual property strategy.

## Why patent protection for cloud-based inventions?

Cloud computing in itself is not a new concept, but following the definition by the United States National Institute of Standards and Technology, 2011, is a system that allows on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services). The technical foundation of the cloud is the presence of a "hypervisor" and the ability to respond to changing demands of the computing environment by automation. The automation allows for existing "virtual machines" to be moved and for new virtual machines to be created on demand. Software installation and configuration is also automated so that when a new virtual

**Cite this Article as:** Susan Keston (2014)," Cloud Cover: Protecting Innovations", Journal of Cloud Computing , Vol. 2014 (2014), Article ID 683295, DOI:10.5171/2014.683295

machine instance is created, it can then automatically be deployed as a resource by the cloud system.

The features that distinguish a cloud computing system from a standard computer network system when considering patent cover for cloud innovations are: (i) the high level of fluidity in the deployment of software modules of a cloud software system; and (ii) the likely distribution of the underlying cloud computing hardware across multiple jurisdictions potentially under the control of multiple cloud service providing entities. In terms of the form of intellectual property protection for innovations, to intellectual property professionals the implementation of innovations in the cloud gives rise to considerations of the adequacy of copyright protection for software innovations and the availability of patent protection for computer-implemented inventions.

With regard to copyright in the United Kingdom, computer programs are treated as a literary work, so that copyright will subsist if the program is an original literary work: as specified by Sections 1 and 3(1)(b)of the Copyright Designs and Patents Act (1988), the "CDPA". The owner of copyright in a computer program has the exclusive right to copy the work (i.e. to reproduce the work in any material form) or to make an adaptation of the work or any substantial part thereof: sections 16 and 17 CDPA. In the UK legal case of Ibcos Computers v Barclays Mercantile Highland (1994), the judge dealt with the proper approach to copyright infringement in computer programs. The UK legal case of Cantor Fitzgerald v Tradition (2000), the judge noted that it is generally accepted that the "architecture" of a computer program is capable of protection if a substantial part of the programmer's skill, labour and judgment went into it.

A commonly-held view in the computer programming community is that copyright alone generally offers sufficient legal protection for an innovative computer program, and provides an adequate remedy against a competitor copying the idea without permission. However, there are some potential pitfalls of adopting a strategy of exclusive reliance upon copyright to protect computer program innovations. In particular, copyright law is jurisdiction dependent. In the UK, copyright protection is limited to the expression of an idea and so would not cover, for example, an independently written version of a piece of program code, even though the same functionality might be provided. Thus, copyright alone is unlikely to offer sufficient breadth of legal protection for an innovative computer program that provides a technical solution to a problem, but which could be coded in multiple different ways. However, copyright may protect a particular 'expression' of computer program code in which the invention is implemented. In short, copyright protects "form" whereas patents protect "substance".

Patents for computer-implemented inventions are in fact available in Europe despite a legal exclusion in Article 52(2)(c) and Article 52(3) of the European Patent Convention (EPC) from patentability for computer programs *"as such"*. In practice, if a "further technical effect" can be demonstrated and an invention meets other patentability criteria (e.g. being new, non-obvious and industrially applicable) then a patent for a computer-implemented invention should be granted by the European Patent Office (EPO). This followed from the EPO Technical Board of Appeal decision (T1173/97 1998) Computer program product/IBM, which is a landmark decision for the patentability of computer-implemented inventions. A summary of the developments concerning patentability of computer programs under the European Patent Convention is given in (EPO Enlarged Board of Appeal decision G3/08, 2010) as a response to questions filed by the President of the European Patent Office according to Article 112(1)(b) EPC. Further key EPO Technical Board of Appeal Decisions pertinent to the patentability of computer implemented inventions include: T769/92 (1994) General-purpose management system/SOHEI, T641/00 (2002); Two identities/Comvik, T154/04 (2006); Estimating sales activity/Duns Licensing

Associates; and T1227/05 (2006) Schaltkreis simulation/Infineon Technologies.

In the United States, patentability criteria are codified in the U.S. Patent Act 35 United States Code (U.S.C.) §101. In the landmark U.S. Supreme Court decision Diamond v. Chakrabarty (1980), the court stated that interpretation of U.S.C. §101 should be such that patent protection should extend to *"anything under the sun that is made by man"*. This led to the U.S. being considered to have a generally more permissive approach to patentability of computer-implemented inventions than Europe. However, more recent U.S. court decisions of Mayo v. Prometheus (2012) and Bilskiv. Kappos (2010) have limited the *"anything under the sun criteria"*. The Tysver (2013) BitLaw blog article provides a detailed overview of the current U.S. case law.

Cloud service providers should be aware that there could be scope for a potential competitor to sign up to a cloud service for a limited period in order to gain access to source or object code associated with a cloud-based service and to then use the information gleaned to set up a competing cloud-based service. Since copyright protects only the form of the program code (both source code and object code) and not the substance of its technical function, the cloud service provider would be well-advised to seek patent protection for its own cloud-based innovations. This patent protection could then be used, upon grant of the patent application, to dissuade a competitor from implementing the invention in the jurisdictions covered or at least to require that competitor to share any rewards from implementing the patented technology.

A set of patent claims serves to delineate a justifiable monopoly for a computer-implemented invention relative to the known state of the art at the priority date. To establish whether a competing product infringes a patent, the court will look to the patent claims to establish whether or not an alleged infringing product falls within their scope. It is very important that a claim set for a patent application is carefully drafted to obtain the best possible scope of protection available to the patentee given what is already known. This is likely to present additional challenges in view of the dynamic architecture of cloud systems. The filing of a patent application has the advantage of allowing the patent applicant to capitalise on the innovation disclosed in that particular application, for example, via licensing and, upon grant of the patent, to prevent competitors from exploiting the invention without the consent of the patent proprietor.

### *Enforcement of Cloud-based Patents*

The territorial nature of patents, which are enforced at the national level, can present some challenges for enforcement of a patent claim that is directed to an entire cloud-based system. This is because the cloud client could be in one jurisdiction, the cloud processing hardware and applications could be in a second jurisdiction under the control of a main cloud service provider contracted by the cloud client and the storage of data required for implementation of the invention could be cloud storage located in a third jurisdiction, possibly in the hands of a party sub-contracted by the main cloud service provider. How can this complexity be addressed to adequately protect a company's investment in cloud innovation?

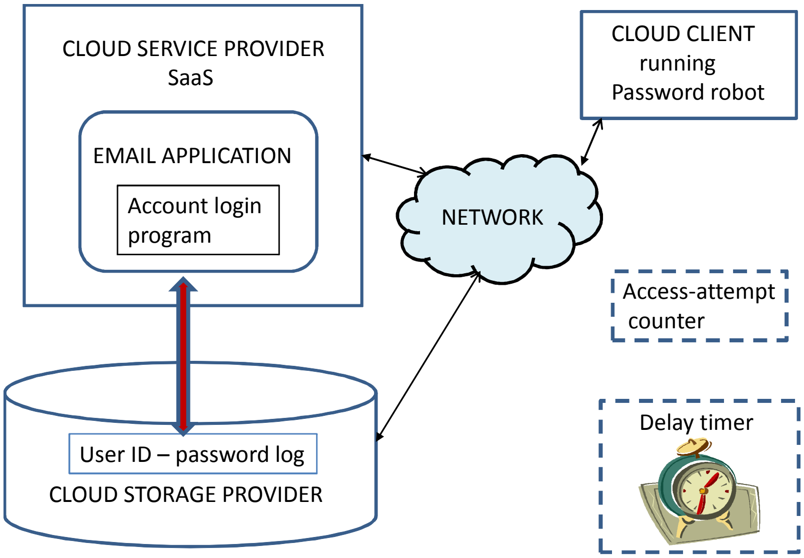

**Figure 1: Illustrative example of cloud-based invention**

Figure 1 provides an example of a potentially patentable cloud-based “invention”. The invention represents a solution to the technical problem of preventing unauthorised access to a user account in a cloud-based email application service from being compromised by a “password robot” running on the machine of a rogue cloud client. The password robot is configured to cycle through thousands of potential passwords based on dictionary words in an attempt to gain unauthorised entry to an email account.

The solution offered by the invention of Figure 1 is to implement a progressively longer delay between successive failed login attempts to a given email account. In the cloud-based email application, a cloud service provider offers the email as a Software as a Service (SaaS), but outsources password storage for user accounts to a third party cloud storage provider. Implementation of the invention requires (i) an access attempt counter; and (ii) a delay timer. These two system components can be instantiated either on the cloud service provider hardware or the cloud storage provider hardware, depending upon implementation preference. To consider how such a system can be adequately protected by one or more patents, a basic understanding of how infringement is approached from a legal perspective is essential.

### *Direct and Indirect Infringement*

Currently, although a European patent route (via the European Patent Office) and a worldwide patent route (under the Patent Cooperation Treaty of the World Intellectual Property Organization) are available, infringement and validity of a patent is still a matter for national law, although there are some similarities between different jurisdictions. For example, there are generally provisions for both direct infringement and indirect infringement, with the criteria for assessing them being jurisdiction-specific. Generally, direct infringement is more straightforward to establish than indirect infringement.

In the UK, direct infringement is legally defined by section 60(1) of the UK Patents Act 1977, whilst indirect infringement is defined by section 60(2).

Direct infringement in the UK can be established if a single party (e.g., a cloud client or a cloud service provider) performs an act or acts such as manufacture, sale or use, which falls directly within the scope of a given patent claim, with no other party being involved in the infringing act. In the context of cloud computing, the difficulty is likely to be claiming an inventive aspect of, for example, a particular cloud architecture, in a way that makes infringement of a given claim by a single party likely. Even an inventive computer program could be executed on cloud hardware of more than one party in a way that could be difficult to capture during patent enforcement. Furthermore, direct infringement of a method claim requires knowledge on the part of the alleged infringer to be demonstrated, which is not required for an apparatus claim, so this sets a slightly higher barrier for enforcement of method claims.

Indirect infringement allows for a patent to be enforced against a single party when more than one party is contributing to a given allegedly infringing act. In the example of Figure 1, the cloud service provider and the cloud storage provider may have to be implicated together in an alleged infringement of a claim to a computer program product covering the email login application using the progressive time delay. Thus, it is clear that indirect infringement is likely to be highly relevant in the cloud computing arena where multiple parties co-operate to perform computing services. Indirect infringement involves a legal entity (single party) supplying *"any of the means relating to an essential element of the invention, for putting the invention into effect in the UK"*(from section 60(2) UK Patents Act 1977) and requires knowledge on the part of the alleged indirect infringer that those "means" are intended to put the invention into effect.

One important consideration, in the case of cloud-based inventions when considering making a case for indirect infringement of a patent claim is the requirement to show that the alleged infringer has put the invention *into effect in the UK.* This could potentially present difficulties in cases where, for example, an essential feature of the invention is implemented on a computer outside the UK. However, there is evidence that the UK Courts are rising to the challenge of applying traditional patent law in the dynamic technological environment of distributed computing in a way that prevents an alleged infringer from evading infringement through such a technical jurisdictional argument.

In the patent case of Menashe v William Hill heard by the Court of Appeal in 2002, Menashe alleged indirect infringement of its patent to an internet betting system by William Hill in supplying its customers with means to put the invention into effect. The Menashe patent claim was to an overall system comprising: a host computer (server), terminal computers and a computer program enabling a terminal to operate the system. William Hill's system offered a similar betting system to the British public via their personal computers from a server located overseas in Antigua, the computer program being generally supplied on a CD-ROM for installation by a client on their own computer. Of course computer technology advances much more rapidly than the law, with the use of CD-ROMs for software installation having already been superseded by downloading.

William Hill denied that its gaming system fell within the scope of the patent's claims, alleging non-infringement on the basis that the host computer in question was situated not in the United Kingdom, but in Antigua. In this case, a broad interpretation of indirect infringement under s60(2) was upheld by the Court, which decided that the *use* of the whole claimed system was effectively in the UK regardless of where the host computer was located because the location was not important to the user of the invention or to the claimed gaming system. This judgement is encouraging when considering the prospect of enforcing a patent claim to cloud-based technology by alleging indirect infringement.

The article by Thornham (2013) provides an interesting discussion of the enforcement of patents regarding cloud computing from a UK perspective. The article by Cordell (2013) discusses infringement liability in cloud-based systems with an emphasis on copyright.

Of course jurisdictions other than the UK ought to be considered with regard to cloud-based patent infringement. In the United States of America (U.S.), there is further evidence of patent law being adapted by the courts to face up to the challenges of adequately protecting cloud computing inventions. In August 2012, the U.S. Court of Appeals for the Federal Circuit ruled in the cases of *Akamai Tech., Inc. v Limelight Networks, Inc. and McKesson Tech. Inc. v Epic Systems Corp.* to the effect that inducing infringement may be found even where multiple entities perform the claimed method steps. This replaces a long-standing single-entity rule in the U.S. for proving direct infringement underlying an inducement claim. The article by Galli (2012) discusses U.S. infringement law in more detail.

### *Claiming the cloud – a strategic plan*

Although indirect infringement *can* be established by a patent holder, it may not be easy to do so. Thus in a cloud-based system, like the example system of Figure 1, to increase the likelihood of direct infringement, ideally independent claims should be drafted from multiple perspectives. A first independent claim could be drafted to capture the steps of the invention directly performed by the cloud client; a second independent claim could be drafted to capture steps of the invention performed by the main email Software as a Service (SaaS) Cloud Service Provider; a third independent claim could be directed to the actions performed by the Cloud Data Storage provider; and a fourth independent claim could cover the whole system. Apparatus claims drafted in this modular way provide a good basis for enforcement via direct infringement. Method claims, which can be potentially broader in scope, provide a good back-up, although as noted above, enforcing a method claim, even against a single party, requires knowledge on the part of the alleged infringer to be demonstrated.

In the system of Figure 1, the main software implementing the invention is part of the account login program application running on the Cloud Service Provider hardware. However, that email login algorithm requires input from the access-attempt counter and the delay timer, which could be located either on the Cloud Service Provider or on the Cloud Storage Provider. Drafting of patent claims should take careful account of these alternatives. The characteristic scalability and extensibility of cloud systems mean that cloud systems are much more dynamic than more traditional computing systems and careful account should be taken of this by the patent draughtsperson, who will require a good understanding of the cloud architecture to creatively protect possible alternative implementations of an invention.

Furthermore, the login algorithm is effectively “used” in the Menashe (2002) sense at the cloud-client side where the increasing delays between successive attempted logins are apparent via the cloud-client interface. Thus, an independent claim to the client would be appropriate and would have the additional advantage of being more easily discoverable from an infringement detection perspective.

It should be noted that whilst the end user is typically not considered to be a good target for patent enforcement, cloud computing is different because the “user” of a cloud service may well be an enterprise serving a large pool of users rather than a lone private individual.

### *Inventions generated collaboratively between Cloud Service Provider and Cloud Client*

In cloud-based systems, there is the scope for an inventive solution to a cloud-based technical problem to be generated collaboratively. For example, a cloud service provider might implement an inventive new cloud interface for a cloud client responsive to a cloud client’s feedback, contributing in the process a partial solution to a technical problem with the pre-existing interface. Could the Cloud Service Provider then proceed to offer that same improved interface to a direct competitor of the Cloud Client without the express permission of the Cloud Client? Similarly, if a Cloud Client modifies and enhances, in a new and inventive way, a software application written by the Cloud Service Provider and made available to the Cloud Client via a cloud-based service, what rights does the Cloud Client have to that invention?

For an inventor resident in the UK, ownership of intellectual property will be governed by the UK law. Generally, the UK law will govern ownership of these rights for the UK resident worldwide. In the UK law, ownership of an invention is governed by Section 7(2) Patents Act 1977, which provides that a patent for an invention is owned by the inventor or inventors; or by any person who is entitled to the inventors' rights by virtue of employment, contract or otherwise.

Contractual terms could be included in a cloud service contract to clarify the status of an invention developed in a collaborative manner by cloud client and cloud service provider to avoid any subsequent misunderstandings with regard to invention ownership and/or commercialisation. Co-ownership of an invention under statute, where there is no overriding contractual agreement, can often be problematic. Under the UK law, for example, a co-owner of a patent can use the invention and sue a third party for infringement of the associated patent without the consent of the co-owner. However, a co-owner of an invention would require permission from other co-owners in order to assign or grant a licence to a patent for the invention.

## Entrusting Data and Software related to other Technology Fields to the Cloud

Thus far, the discussion of cloud-based innovations has centred upon innovations in the technical field of cloud-computing itself. Now, we shall consider using cloud-based technology to store data relating to inventions in other technical fields and using cloud platforms to develop software for which patent protection may be sought. For example, invention disclosure data for inventions in the pharmaceutical field could be entrusted to cloud storage or a software application related to a new type of audio encoding could be developed using a cloud-based platform. An informative discussion, which considers different considerations for data generated inside the cloud and data generated outside the cloud, can be found in the article by Reed (2010).

The Paris Convention for the Protection of Industrial Property Articles 4A to 4I provides that when a patent application is first-filed in one country party to the Paris Convention, the applicant is entitled to claim priority for a period of twelve months and the filing date of that first application is considered the “priority date." Therefore, when patent protection is subsequently sought for the same invention by filing patent applications in member countries of the Paris Convention during those twelve months, priority can be claimed from the first-filed application so that the subsequent applications benefit from having the same priority date: the priority date is thus the effective filing date for the subsequently filed applications relating to that invention.

There is a requirement for worldwide novelty (see, for example, Patent Cooperation Treaty, Article 33(2) and Rule 33.1(a)) of an invention at the “priority date” of a patent application as a prerequisite to obtaining patent protection. This absolute novelty requirement means that there is a need to safeguard inventions against inadvertent public disclosure prior to the filing of the first patent application.

Considering the example of the innovative audio encoding algorithm being developed on the cloud, if the cloud service provider made the algorithm accessible to cloud clients other than the inventing entity or made the algorithm available to a cloud sub-contractor prior to a patent application being filed, these acts could mean that the subsequently-filed patent application does not fulfil the novelty requirement. The same is true if the invention disclosure data for pharmaceutical products is made available to third parties via cloud-based storage prior to a patent application being filed.

Some safeguards in law against inadvertent disclosure are available in many jurisdictions, which provide for grace periods for filing a patent application where there has been a disclosure of the invention in breach of confidence. However, the detailed criteria for qualifying for the grace periods differ for each country so a careful assessment by a patent professional is required of whether or not they are fulfilled in a given case. In most countries, the grace period applies to disclosures made by the inventor and not by third parties. In the case of a European patent, Article 55(1) EPC provides that the application must be filed within six months of the disclosure in order to benefit from the non-prejudicial disclosure provision. However, this provision should not be relied upon because the case law sets a high threshold for demonstrating that such a breach has occurred. The UK and Japan also have 6 month grace periods and there is a limited 12 month grace period in the US.

In a cloud computing environment, potentially spanning multiple countries, it is likely to be more difficult to ascertain within the grace period that there has been an unauthorised disclosure of the invention and to file the patent application in time for the disclosure to be categorised as non-prejudicial. Furthermore, the chain of responsibility for breach of confidence could be more difficult to establish in a complex cloud-based system where, for example, the unauthorised disclosure of documentation relating to a cloud client's invention was made by a data storage provider sub-contracted by the client's cloud service provider and where there was no direct contractual relationship between the data storage provider and the cloud client. It is likely to be difficult to prove that the disclosure in breach of confidence was made directly or indirectly by one of the inventors.

Provided the cloud client understands where the cloud service provider is holding the commercially sensitive information; and who has access to it, there is no reason why the opportunities afforded by the cloud to facilitate innovation in other technical fields should not be taken full advantage of. An awareness of the absolute novelty requirements with regard to patents should allow an objective decision to be made regarding whether or not to entrust intellectual property to the cloud.

### ***Straight to the Cloud after Patent Application Filed?***

Once a patent application has been filed for an invention, unauthorised disclosure of the invention via the cloud should be of less concern. However, patent applicants should be aware that they could potentially be putting information into the public domain that would otherwise not be available until publication of the patent application, typically 18 months after filing.

There is also need to protect against inadvertent disclosure of any improvements or refinements of an invention if those improvements/refinements have been omitted from the patent application as filed. Thus, for example, further development of the audio encoding algorithm application software for which a patent application has already been filed could be undertaken by running and fine-tuning the code on a cloud-based platform. However, in the absence of appropriate security provisions to prevent unauthorised third parties from accessing and/or disclosing the software under development, filing of one or more further patent applications directed to independently patentable refinements of the invention could be compromised in terms of absolute novelty.

### *Safeguarding Intellectual Property via the Cloud Contract Terms*

When signing up to a cloud service contract, potential cloud clients ought to consider the safeguarding of their own intellectual property and their potential liability for infringement of third party patents as being just as important as the criteria of cost-effectiveness and performance. The article by Kuan Hon (2012) provides a detailed discussion of considerations to be made when negotiating cloud contracts.

If intellectual property is to be located in a remote jurisdiction via the cloud then local intellectual property law, for example, with regard to disclosure of an invention in breach of confidence, should be reviewed.

## Software Licensing

A Cloud Service provider may not own intellectual property rights in software offered via SaaS to a cloud client. Software licences are generally restricted licences for the purchaser to use the particular program code and, as such, are primarily copyright waivers. However, many "shrink-wrap" software licences distributed with computer program applications also include a licence under any patent applications proprietary to the software vendor. Software licenses are traditionally territorial in character whereas in cloud computing environment, the cloud service architecture could mean that the software is being executed in a different jurisdiction from the jurisdiction in which the user is accessing the software. It could be argued that following Menashe v William Hill (2002), the place where the invention is used is the important factor, at least from the point of view of patent infringement, but the success of this argument cannot be guaranteed.

Cloud clients should check whether the cloud service provider is entitled to sub-license any software for which the cloud service provider holds a software licence to the cloud client. Alternatively, there may be provision for a direct licence between the intellectual property holder and the cloud client. The cloud client should establish a clear understanding of their potential liability for infringement of a patent held by a third party under the terms of their cloud service contract. Any intellectual property indemnity provided as part of a cloud service contract ought to protect a cloud client in each jurisdiction in which the software is likely to be used. Corporate software licenses often carry a limit upon a number of concurrent users permitted under the terms of the licence. This could be difficult to track in a cloud-based system.

## Free and Open Source development in Cloud Computing

Free and Open Source Software (FOSS) is a fundamental component of current computing technology and has an important role in driving software-based innovation and development. Software patents and Open Source development have both experienced excellent growth in recent years, as evidenced in the case of Open Source by the paper of Riehle(2008), suggesting that there is not, as has been suggested by some, a negative correlation between the number of software patents granted and the uptake of Free and Open Source software.

However, there are some potential pitfalls to be aware of when utilising FOSS software in a cloud computing environment. FOSS can in some cases interact with intellectual property rights in a way that is potentially detrimental to a company incorporating FOSS in a commercial software product.

Many cloud service providers build cloud services and even cloud platforms using FOSS. Both cloud clients and cloud service providers should be aware that Open Source licences can vary considerably in terms of their obligations upon the licensee. Depending upon the terms and conditions of an Open Source licence, a cloud client/provider could be placed under an obligation to divulge source code comprising Open Source software to third parties and could unintentionally be giving an implied patent licence by distributing software comprising an Open Source component. The OSS Watch website provides a useful explanation of the terms of a number of different Open Source languages in plain English and provides a basis for comparison.

Depending upon the business model of the software provider for the particular software product, the Open Source obligations may not be problematic and could even be advantageous. This would be the case, for example, where the originator of the derived software has a market in services relating to the software or where widespread uptake of the software by a technology sector would be likely to provide a boost to sales of associated proprietary hardware and/or software. However, the obligation could pose a problem if one Cloud Service Provider was obliged to divulge the full source code for a key cloud-based service to competing Cloud Service Providers, even if that full source code only incorporated Open Source software for a small proportion of the total number of program functions and the remainder of the source code was generated via expensive in-house research and development.

In the UK, Open Source licenses remain largely untested to date in terms of enforcement and they have been tested in the US with limited success. It could be difficult for the Open Source licensor to establish that Open Source program code is present in a "black box" product, particularly where the Open Source code comprises a minor component of the software product. Nevertheless, the potential consequences of breaching the terms of an Open Source licence agreement should not be disregarded, because it could lead to a requirement to publish source code. This could be detrimental commercially depending upon the timing of the enforced disclosure and the market share of the product at that time.

## Conclusions

Cloud computing is a fertile ground for innovation in the technical field of cloud computing both on the part of the cloud service provider and the cloud client. The innovator would be well advised to carefully devise an intellectual property protection strategy that will meet the new challenges presented in this field, while other stakeholders in cloud technologies should also consider how their competitors may be taking advantage of available protection with a view to future exploitation and possibly enforcement.

The cloud also offers exciting opportunities to drive forward innovations in technical fields other than cloud computing, (e.g., audio/video encoding, electronic payment security, genetic engineering etc.) taking advantage of a cloud computing platform to harness expandable processing power and data storage capability. An awareness of how to safeguard against inadvertent public disclosure of inventions via the cloud before adequate patent protection is in place should allow full advantage of cloud technology to be taken by a business, without compromising an intellectual property protection programme.

## References

Akamai Tech., Inc. v. Limelight Networks, Inc., and McKesson Tech., Inc. v. Epic Systems Corp., 692 F.3d 1301, 1306 (Fed. Cir. Aug. 31, 2012).

Bilski v. Kappos, (2010), 130 U.S. Supreme Court, 3218, 3231.

Cantor Fitzgerald v Tradition (UK) (2000),*Reports of Patent, Design and Trade Mark Cases(RPCs)* 95, at paragraphs 76-79, Pumfrey J.

Diamond v. Chakrabarty, (1980), 447, U.S. Supreme Court, 303.

Cordell, N., (2013), 'Intellectual Property in the Cloud', Allen & Overy, [Online], [retrieved September 18, 2013],http://www.allenovery.com/ SiteCollectionDocuments/Intellectual_property_in_the_cloud_May_2013.PDF.

European Patent Office, *"Guidelines for Examination"*, Part G Chapter III, section 3.6 "Patentability: Programs for computers", [online] [retrieved September 18, 2013],

http://www.epo.org/law-practice/legal-texts/html/
guidelines/e/g_ii_3_6.htm.

Galli, N. D. and Gecovich, E., (2012), "Cloud Computing and the Doctrine of Joint Infringement: 'Current Impact' and Future Possibilities", *The John Marshall Review of Intellectual Property Law*, 11, page 673.

Ibcos Computers v. Barclays Mercantile Highland (1994),*Fleet Street Reports*, 275.

Kuan Hon, W., Millard, C.and Walden, I. (2012), "Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now", *Stanford Technology Law Review* 16, page 81, [online], [retrieved September 21, 2013], http://stlr.stanford.edu/pdf/
cloudcontracts.pdf.

Mayo v. Prometheus (2012), 132 Supreme Court 1289, [online], http://www.supremecourt.gov/opinions/11pdf/10-1150.pdf.

Menashe Business Mercantile Ltd.&Anor v William Hill Organization Ltd. [2002] EWCA Civ. 1702, [2003] 1 All ER 279, [2003] 1 WLR 1462, [2003] RPC 31 (28 November 2002), Court of Appeal.

National Institute of Standards and Technology, NIST (2011) "The NIST Definition of Cloud Computing" SP800-145.pdf [Online], [Retrieved May28, 2013], http://csrc.nist.gov/publications/PubsSPs.html#800-145.

OSS Watch website (2013), "Open Source Licences", [online], [retrieved September 21, 2013], http://www.oss-watch.ac.uk/resources/licencefinder.

Paris Convention for the Protection of Industrial Property (1883, as amended 1979),Articles 4A to 4I, "Patents, Utility Models, Industrial Designs, Marks, Inventors' Certificates: Right of Priority" [online], [retrieved September 18, 2013], http://www.wipo.int/treaties/en/ip/paris/.

Riehle, D., and Deshpande, A.(2008) "The Total Growth of Open Source",*Proceedings of the Fourth Conference on Open Source Systems*. Springer Verlag, Page 197-209. [online] [RetrievedJune 2, 2013], http://dirkriehle.com/publications/2008/the-total-growth-of-open-source/.

Thornham, C., (2013) "Get off my cloud", *Intellectual Property magazine*, May 2013, pages 57-58.

Tysver, D. (2013), "The History of Software Patents: From Benson, Flook, and Diehr to Bilski and Mayo v. Prometheus", BitLaw Blog, [online], [Retrieved September 21, 2013], http://www.bitlaw.com/software-patent/history.html.

T 769/92 (1994), "General-purpose management system/SOHEI", *Official Journal of the European Patent Office* 8/1995, page 525.

T 1173/97 (1998), "Computer program product/IBM", *Official Journal of the European Patent Office* 10/1999, 609, [online], http://www.epo.org/law-practice/case-law-appeals/recent/t971173ex1.html.

T 641/00 (2002), "Two identities/COMVIK", EPO Technical Board of Appeal Decision, [online], http://www.epo.org/law-practice/case-law-appeals/recent/
t000641ep1.html.

T 258/03, (2004), "Auction Method/HITACHI", EPO Technical Board of Appeal Decision [online], http://www.epo.org/law-practice/case-law-appeals/recent/
t030258ep1.html.

T 154/04, (2006), "Estimating sales activity / DUNS LICENSING ASSOCIATES", EPO Technical Board of Appeal Decision, [online],http://www.epo.org/law-practice/case-law-appeals/recent/t040154ep1.html.

T 1227/05, (2006) "Schaltkreis simulation/ INFINEON TECHNOLOGIES", EPO Technical Board of Appeal Decision, [online],http://www.epo.org/law-practice/case-law-appeals/recent/t051227ep1.html.

UK patents Act 1977 section 60, Meaning of Infringement; available from the UK

Intellectual Property Office website; http://www.ipo.gov.uk/patentsact1977.pdf.

## Bibliography

European Patent Convention 2000, 14th Edition, 2010, [Online], [Retrieved September 18, 2013], http://www.epo.org/law-practice/legal-texts/html/epc/2010/e/index.html.

European Patent Office, [online],http://www.epo.org/.

Patent Cooperation Treaty, as in force from April 1 2002, [Online], http://www.wipo.int/pct/en/texts/articles/atoc.htm.

Patents Legal Section UK Intellectual Property Office "Patents Act 1977 (as amended) 1 October 2011, An unofficial consolidated version", [online], [Retrieved September 18, 2013], http://www.ipo.gov.uk/patentsact1977.pdf.

Queen Mary, University of London Cloud Legal Project, [online], http://www.cloudlegal.ccls.qmul.ac.uk/index.html.

The United States Patent and Trade Mark Office, [online], http://www.uspto.gov/.

United Kingdom Intellectual Property Office, [online], http://www.ipo.gov.uk/.

United Kingdom Intellectual Property Office "Patents Act 1977: Patentability of computer programs" December 8, 2008, [online], http://www.ipo.gov.uk/pro-types/pro-patent/p-law/p-pn/p-pn-computer.htm,

World Intellectual Property Organization, [online], http://www.wipo.int/ patentscope/en/.