Intellectual property in the cloud

May 2013

www.allenover.com
Intellectual property in the cloud

While market research firms consistently predict spectacular growth in year-on-year spend on cloud-based technology, intellectual property issues in the cloud continue to be one of the “cloudiest” legal areas for customers and suppliers alike. What case law there is is relatively new and untested, leading David Jones, Microsoft’s Associate General Counsel for IP Policy, to conclude at last year’s AIPPI Congress in Seoul that trying to decide how cloud IP issues will resolve is much like “trying to read the tea leaves”.

Cloud computing in itself is not new. However, due to the global and often complex nature of the services, existing legal challenges may be amplified. This is particularly the case with intellectual property, where IP commentators have long suggested that IP policy is failing to keep pace with technological developments. In this article we identify some of the possible IP hot spots (with a particular focus on UK copyright issues), and offer suggestions to mitigate risk in what is a very rapidly evolving area of law.
Enforcing IP rights in cloud-related technologies

One issue for those seeking to protect and enforce rights to cloud-related technologies is to identify whether or not the technologies are patentable. Approaches to software and business method patents vary significantly by jurisdiction. In the UK, for example, the Intellectual Property Office takes a fairly restrictive approach to what is patentable when compared to the more lenient U.S. regime.

In any event the decision whether or not to seek patent protection is in itself not straightforward. A patent application requires disclosure of the detail of the invention and this may benefit competitors (particularly if the application is unsuccessful). While the wheels of the average patent office may turn slowly, software iterates quickly, and commercial lifecycles are relatively short. In a cloud computing environment, companies may be better advised to take advantage of the cloud as a way of hiding their technology from competitors and focus instead on first mover exclusivity in the market and the protections afforded by copyright and the implementation of robust approaches to defending trade secrets.

It is this ability to “hide” technology behind the cloud (particularly for vertically integrated companies) that can also make enforcement of IP rights challenging. When a software company suspects that a competitor is infringing a patent, reverse engineering to prove an infringement may not be possible in a cloud environment where the “nuts and bolts” stay on the provider’s servers.

Ownership of newly-created content

In the course of uploading, storing and processing the customer’s data, the cloud service provider (“CSP”) may create new IP. The most obvious examples of this in practice will be database rights and copyright, with the latter being the main focus of this article. This new IP may be difficult to separate from the existing content (particularly where, for example, the customer might develop the application while the CSP contributes the platform, or where the CSP arranges and presents the customer’s data in a certain manner after the data is uploaded) and it may also be difficult to identify the owner of such IP.

In the absence of an express assignment, it is likely to be the CSP which owns the rights in the UK (and indeed some standard terms do state that CSPs own new content created). There is also the potential for joint ownership of copyright in new content if it is produced by a collaboration between the CSP and customer and the contribution of each is not distinct from that of the other (s. 10(1) Copyright, Designs and Patents Act 1988 (“CDPA”)). The contribution of each must be significant for there to be joint ownership,¹ and there is no requirement for an intention to create a work of joint ownership, with acting pursuant to a common design being sufficient.² Where new content is jointly owned by the CSP and customer, neither is able to exploit the work without the consent of the other. Therefore, assuming a customer wishes to own and/or use the newly created IP, it is important that they either: (i) obtain an express assignment of the newly created IP; or (ii) get the full licence rights they need to use the newly created IP. These terms need to take into account what happens to ownership or assignment after the termination of the cloud arrangements.

New IP can also come about from work product of the services provided through the cloud, for example, bug fixes or service improvements that arise as a consequence of customer suggestions or customisations that a user may

¹ Pierce v (1) Promco SA [1999]
² Beckingham v Hodgens [2003]
deploy in the context of a PaaS or IaaS arrangement. Ownership can be particularly relevant in this context where the customer may not wish a competitor who also uses the cloud services to have the benefit of the same improvements.

Cloud services may create metadata about the customer’s use of the service and this can be very useful to third parties and a potential source of revenue for the CSP. These rights are likely to be owned by the CSP, but where information relates to a specific customer the data is likely to be confidential. Service terms should address creation, ownership and use of such data including questions of aggregation and anonymisation.

Liability for copyright-infringing content uploaded onto the cloud

Given the vast number of services which are provided in the cloud, there are plenty of different ways in which copyright-infringing content can be uploaded onto the cloud. Let's take for example a cloud storage system where users can upload music, videos, photos or documents. What happens when copyright works are uploaded onto such a service?

Individual liability

The position on liability for an individual user varies from jurisdiction to jurisdiction. In the UK it is a primary infringement to copy a copyright work in any material form, which includes storing the work in any medium by electronic means (s. 17(2) CDPA), and it is generally the person who makes the copy (ie the individual user) who infringes copyright, rather than the owner of the machine on which the copies are made. Across most of Europe there is an exception to copyright infringement to allow the making of copies for private use or for format shifting.

However, this is not universal. It does not exist under current UK copyright law, although in December 2012 the UK Intellectual Property Office stated the intention to introduce a new “private copying” exception into UK law later this year to enable “a lawful owner or buyer of a copy of a work to reproduce that copy for their personal use”. Importantly, it “sees no reason in principle” why this “narrow” and “technology-neutral” exception should not apply to digital content stored on cloud computing servers.

There is also an additional question as to whether a copyright owner would choose to take action against the individual user given the number of individuals who undertake this sort of copying.

Primary liability of the CSP

As a matter of UK law, the question of whether there is any liability for the CSP will turn on the specific facts of the case. As stated above, it is generally the person who makes the copy (ie the individual user) who directly infringes copyright, rather than the owner of the machine on which the copies are made. On this basis, the CSP would be unlikely to be primarily liable for performing the act of copying. It is, however, important that it is the user’s decision to upload the copyright material.

However, assuming the individual customers would be committing copyright infringement, the copyright owner may seek to argue that that CSP is primarily liable for authorising the acts of copying (s. 16(2) CDPA).

Authorisation is where someone grants or purportedly grants the right to a user to undertake an infringing act. The Newzbin case involved a website operated by Newzbin Ltd which provided a search facility and hyperlinks to another website on which users could download unlawful copies of films. The High Court held that Newzbin infringed the copyright in a number of films.

---

2 Twentieth Century Fox Film Corporation, Universal City Studios Productions LLLP, Warner Bros. Entertainment Inc., Paramount Pictures Corporation, Disney Enterprises, Inc., Columbia Pictures Industries, Inc. v Newzbin Limited [2010] EWHC 608 (Ch) (1-3, 8, 10 February, 2, 3 March 2010), High Court (England and Wales)
by authorising its users to illegally copy those films.

In assessing whether an entity authorises the infringing acts of its users, there are a number of factors to take into account, including:

– the nature of the relationship between the alleged authoriser and the primary infringer;
– whether the equipment or other material supplied constitutes the means used to infringe;
– whether it is inevitable that these means will be used to infringe;
– the degree of control that the alleged authoriser maintains; and finally
– whether the supplier has taken any steps to prevent infringement, such as displaying a prominent notice to users stating that the service is not to be used to create unauthorised copies of third party copyrighted material.

However, such notices must not be “purely cosmetic”, ie they must intend to be acted upon, and not a superficial attempt to conceal the true purpose of the website.

In a cloud storage system where users can upload music, videos, photos or documents, the facts that the cloud service can be used for non-infringing purposes and that the CSP retains little control over what content is stored by a user would be factors against a finding of authorisation. But, the question of authorisation will turn on the specific services offered by the CSP.

Assuming the individual customers have committed primary copyright infringement, the copyright owner may also argue that the CSP is liable as a joint tortfeasor where it can be said to have procured the infringement by inducing, inciting or persuading the customer to infringe copyright or where the CSP has engaged in a common design with some of its customers to infringe copyright.

Mr Justice Kitchin held that all the matters which were relevant to the issue of authorisation were also relevant to this issue. So, the arguments on joint tortfeasorship of a CSP would be similar to those for authorisation, and would again turn on the specific facts of the matter.

Secondary liability of the CSP

The copyright owner may also argue that the CSP is liable as a secondary infringer on the basis that, without the licence of the copyright owner, it possesses in the course of a business an article which it knows or has reason to believe is an infringing copy (ie an unauthorised copy of the copyright work uploaded onto its servers) (s. 23(a) CDPA).

On this point we can turn to the Hosting Defence under the E-Commerce Directive (2000/31/EC). Article 14 of the Directive provides that an information society service (any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service) provider which stores information at the discretion of a user (which would include the CSP in the cloud storage system proposed above) will be absolved from liability for that information where:

– it does not have actual knowledge of unlawful activity or information, or awareness of facts or circumstances from which the illegal activity or information is apparent, or, upon being made aware or acquiring actual knowledge, acts expeditiously to remove or disable access to the information; and
– the recipient of the service was not acting under the authority or control of the service provider.

Effectively, this requires the CSP to implement a “notice and takedown” procedure. This means putting in place and acting upon a policy of removing or disabling access to infringing material which is notified to it by the copyright owner. This procedure should be practical and user friendly.
However, in the Google AdWords case\(^4\), the Court of Justice of the European Union (“CJEU”) held that, in order to benefit from this exemption, a service provider has to play a neutral role in the sense that its conduct is merely technical, automatic and passive, thus pointing to a lack of control or knowledge over the data it stores.

The question arises as to whether a CSP should proactively filter users’ material. Article 15 of the E-Commerce Directive provides that there is no general obligation on providers, when providing hosting services, to monitor the information which they transmit or store. Nor is there a general obligation to actively seek facts or circumstances indicating illegal activity. The CJEU in Netlog\(^5\) confirmed that an obligation on a host service provider to filter its entire stored content for infringements of copyright would not be in line with Article 15.

**Injunctions against a CSP**

The exemptions in the E-Commerce Directive, including Article 14, only shield service providers from criminal liability and claims for damages. Consequently, it may be possible to obtain an injunction against a CSP even where it is otherwise exempted from liability under Article 14.

Article 11 of the Enforcement Directive (2004/48/EC) provides that Member States must ensure that rights holders are in a position to apply for an injunction against intermediaries, such as a CSP, whose services are used by a third party to infringe an IP right, as well as against infringers. For example in L’Oréal v eBay,\(^6\) L’Oréal sought an injunction against eBay by virtue of Article 11, even though eBay was not liable for the infringement of its trade mark rights. On referral, the CJEU held that EU law requires Member States to ensure national courts are able to order a website operator to take measures which contribute not only to bringing infringements to an end, but also to prevent further infringements of that kind. Those injunctions must be effective, proportionate and dissuasive, and must not create barriers to legitimate trade.

S. 97A CDPA, which implements Article 8 of the Information Society Directive (2001/29/EC) in the UK, provides the High Court with the power to grant injunctions against intermediaries where it has actual knowledge of a third party using its services to infringe copyright. Article 8 of the Information Society Directive (2001/29/EC) is similar to Article 11 of the Enforcement Directive except that it only applies to copyright, whereas Article 11 also applies to other rights. The 20th Century Fox Film v BT\(^7\) case came soon after the CJEU’s judgment in L’Oréal v eBay in the summer of 2011. An injunction granted in the Newzbin case in 2010 effectively signalled the end for the Newzbin website. However, the website soon reappeared as Newzbin2. This new version of the website used servers located in Sweden, beyond the jurisdiction of the UK courts. A number of film studios subsequently sought an injunction forcing the internet service provider, BT, to block access to the whole of the Newzbin2 site. Mr Justice Kitchin granted an injunction against BT under s. 97A CDPA, requiring it to adopt IP address re-routing and DPI-based URL blocking to block or attempt to block access by its customers to the Newzbin2 website or any other IP address or URL whose sole or predominant purpose is to enable or facilitate access to the Newzbin2 website. This was the first time the High Court granted an injunction compelling an ISP to block or impede access by its subscribers to a website containing copyright-infringing content, and signals that similar measures could be taken in the UK against CSPs.

---

\(^4\) Joined cases: Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08)

\(^5\) Netlog [16 February 2012, C-360/10]

\(^6\) L’Oréal SA and Others v eBay International AG and Others (c-324/09)

Risk of service disruption caused by IP infringement

Though not particular to cloud computing, enterprise adoption of cloud solutions can expose individuals and organisations to increased risk of service disruption because of the variety of software vendors and the remotely distributed nature of the solutions. A good example of this is where the provider is subject to an injunction for IP infringement and there are no readily available alternative technologies.

To protect against this exposure, cloud customers should not view cloud services as an all-or-nothing proposition and should consider if it is useful to retain some degree of skill and resource (staff and computing resources), or even certain business critical functions, internally to protect against service disruption.

Software licensing

Many companies are likely to have built up a variety of software solutions including software offered on-premise, hosted by a third party, provided “as a service” or perhaps hosted through some sort of private/hybrid cloud arrangement. One challenge for cloud customers is to be aware of relevant licensing restrictions or limitations and to manage the plethora of software licensing models that this variety of provision entails. If the basis of the licence fee relates to a fee per workstation (as is common for software provided on site) this may not be easily translated into a virtual application environment where software licence models are often pay-as-you-go and/or subscription-based. Some companies are recognising this challenge and making provision for it. For example, IBM offers a “Bring your own software and licence” arrangement for certain eligible software programmes to be provided via Amazon’s cloud offering.

Another question for cloud customers is who should license the software from the software provider (where that provider is not the CSP). Where third party software is provided over the cloud, the CSP will need to either sublicense software to the customer (preferable), or facilitate a licence between the third party software provider and the customer. In the case of a direct, rather than sub, licence, the CSP should be made contractually liable for software maintenance, and for paying licence fees.

A final consideration is whether software licences authorise software use in all the jurisdictions in which the customer operates or from which the customer may be accessing services from cloud.

IPR indemnities in cloud contracts

To mitigate the risks posed by uncertainty over software licensing, the customer may wish to seek an indemnity for IP infringement. Indemnity may also be sought in relation to the possibility of patent infringement. The customer may also seek indemnity for loss suffered as a result of materials deleted or service disruption. However, it is worth noting that research by staff at the QMUL Cloud Legal Project at the University of London into contract terms for cloud computing arrangements found that, for the most part, CSPs were unwilling to accept liability and instead sought broad exclusion of, or limitations to, their liability.

Market practice at this point indicates that indemnities may therefore be very difficult to negotiate. On the subject of service interruption in particular, customers may do better to focus on service level agreements relating to service availability; and of course to do their due diligence thoroughly on potential providers. Integrators may also be more willing to accept liability.

Should IPR indemnities be successfully negotiated in cloud contracts, they need to be sufficiently broad to protect the intended beneficiary in all jurisdictions in which the service will be used/maintained.
As we have said in previous articles, cloud computing is not new. However, due to the global and often complex nature of the services, existing legal challenges may be amplified. This is particularly the case with intellectual property, where IP commentators have long suggested that IP policy is failing to keep pace with technological developments.

For customers considering a move into the cloud the key questions will be around ensuring that appropriate rights are in place to enable the use of cloud services (eg software licences); identifying the likelihood of content creation through use of cloud services and making appropriate contractual provisions for ownership or assignment of rights (including post termination); and balancing the possible risks of IP infringement and consequential service interruption against the commercial benefits of moving to the cloud.

For cloud service providers critical considerations will turn on how to protect innovations in the cloud, and thinking here should cover the broad range of protections available, including technical and organisational approaches to keeping innovations safe, and the risk of liability for and possibly injunctions to prevent infringing acts by its customers.

The cross-border nature of cloud provision should be an area of particular consideration for both parties, bearing in mind that IP policy is not well harmonised.

Conclusion
Author

Neville Cordell
Partner – London
Tel +44 20 3088 2754
neville.cordell@allenandover.com
Key contacts

Ahmed Baladi
Partner – Paris
Tel +33 1 40 06 53 42
ahmed_baladi@allenovery.com

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Herald Jongen
Partner – Amsterdam
Tel +31 20 674 1614
herald.jongen@allenovery.com

Paul Keller
Partner – New York
Tel +1 212 610 6414
paul.keller@allenovery.com

Will McAuliffe
Partner – Hong Kong
Tel +852 2974 7119
will.mcauliffe@allenovery.com

Filip Van Elsen
Partner – Antwerp
Tel +32 3 287 7327
filip.vanelsen@allenovery.com

Tom de Cordier
Counsel – Brussels
Tel +32 2 780 2578
tom.decordier@allenovery.com

Cyril Pierre-Beausse
Counsel – Luxembourg
Tel +352 44 44 55 515
cyril.pierre-beausse@allenovery.com

Connell O’Neill
Senior Associate – Sydney
Tel +61 2 9373 7790
connell.oneill@allenovery.com

Nigel Parker
Senior Associate – London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Peter Harwich
Partner – New York
Tel +1 212 610 6471
peter.harwich@allenovery.com

Rose Hall
Business Development – London
Tel +44 20 3088 3618
rose.hall@allenovery.com

Charlotte Mullarkey
Senior PSL – London
Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com
GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,000 people, including some 512 partners, working in 42 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi        Düsseldorf        Munich
Amsterdam        Frankfurt         New York
Antwerp          Hamburg          Paris
Athens (representative office) Hanoi
Bangkok          Ho Chi Minh City
Beijing          Hong Kong
Belfast          Istanbul
Bratislava        Jakarta (associated office)
Brussels         London
Bucharest (associated office) Luxembourg
Budapest          Madrid
Casablanca        Mannheim
Doha
Dubai

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP’s affiliated undertakings.

© Allen & Overy LLP 2013 | CS1302_CDD-35340_ADD-37128

www.allenovery.com