Hogan Lovells

Global Media and Communications Quarterly

2015: the year of the website-blocking injunction?

SPRING 2015

Contents

Editorial

Net neutrality is back. At the same time as the FCC was hammering out its new 400-page net neutrality or open internet order, delegations from European Member States were agreeing on compromise language for net neutrality reform in the EU. Yes, the open internet is again in the headlines, with tricky issues like paid peering and zero-rating creating controversy on both sides of the Atlantic. This issue of the Global Media and Communications Quarterly contains an article comparing open internet approaches in Asia, the US and Europe, pointing out some of the fundamental differences between the three regions. Our guest contributors from Analysys Mason look at open internet from the angle of television regulation, focusing on how open internet rules affect the connected TV ecosystem.

Our main article is a multi-jurisdictional study on measures for tackling online copyright infringement, focusing on the rise in successful applications for website-blocking injunctions. More and more courts around the world are issuing blocking orders. Website blocking is of course linked to an open internet insofar as net neutrality rules restrict when ISPs can block content. Typically ISPs must be under a legal obligation, generally a court order, to block.

We also review the recent key developments in new policies coming into force this year, in particular in Spain, Russia and Australia, where the government has announced new initiatives including amendments to the Australian Copyright Act that would allow applications for injunctions requiring ISPs to block access to websites operated outside Australia.

Mexico is one of the fastest moving jurisdictions in the world when it comes to Internet, media and telecoms regulations. In previous issues, we examined Mexico's constitutional reform and new regulatory framework for media and telecommunications. In this issue, we focus on spectrum reform in Mexico, and in particular on Mexico's plans to release further 4G spectrum for existing and new mobile operators.

Recent developments in China include the relaxation of the rules on foreign ownership of e-commerce businesses in the Shanghai Free-Trade-Zone, which came into effect in pilot form in January. In this issue we examine the remaining challenges for foreign investors in China and the real impact of the relaxation of the rules.

Finally, we round out this issue by an article examining the antitrust aspects of standard essential patents, as well as a comprehensive "how to" guide on developing civil UAS (Unmanned Aircrafts Systems) projects. The UAS how-to guide was developed in the context of a UAS conference hosted by our Palo Alto office on 16 April 2015.

Don't forget to visit our www.hlmediacomms.com blog, and sign up to receive notices of new articles in areas that interest you.

Enjoy the reading, and happy Springtime!

Winston Maxwell
Partner, Paris
T +33 1 5367 4847
winston.maxwell@hoganlovells.com

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Penny Thornton
Senior Associate, London
T +44 20 7296 5665
penelope.thornton@hoganlovells.com

Is 2015 the year of the website-blocking injunction?

Internet piracy continues to be a significant problem for rights holders. The creative industries argue that piracy costs the industry £400m a year in lost revenue. In response, several countries around the globe are introducing new regimes to tackle online copyright infringement ("OCI") and at the same time rights holders, dissatisfied with some of the existing national graduated response regimes, are increasingly turning to the powerful and effective tool of website-blocking injunctions. In this article we explore the national regimes for tackling online piracy in some of the key European countries and look at recent important developments both in Europe and in the rest of the world, notably Australia and Russia.

Europe

In 2000 the European E-Commerce Directive[1] established the principle of "notice and take down" procedures, giving ISPs immunity from liability except where they have been notified of infringement and do not promptly take down the content. The following year, the Information Society Directive[2] came into force, which provided that member states must ensure that rights holders can apply for an injunction against internet intermediaries whose services are used by a third party to infringe a copyright. The CJEU confirmed in the 2014 case of *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft*, that Internet service providers ("ISPs") can be ordered to block access by customers to websites making available infringing content and ISPs are free to choose the measures they use provided those measures target the infringing content and do not unjustly interfere with the users' right to freedom of information. The IP Enforcement Directive[3] also requires member states to ensure that measures necessary for the enforcement of intellectual property rights shall not be unnecessarily complicated or costly. The directives had to be implemented through national legislation and this has led to inconsistencies in the national legislation of member states.

UK

In the Government's Review of Intellectual Property in the UK in December 2006 (the Gowers Review) Mr Gowers reported that UK legislation, in particular s97A of the UK Copyright, Designs and Patents Act 1988, was not providing rights holders with sufficient protection against OCI (in particular illegal file-sharing). Under s97A, the High Court has the power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright. Gowers recognised that rights holders and ISPs disagreed over the interpretation and effect of s97A and it was completely untested since 2003. Consequently, in February 2008, the government said it would consult on legislation that would require ISPs and rights holders to co-operate in taking action on OCI, with a view to implementing legislation by April 2009. In July 2008 the UK's six largest ISPs signed a memorandum of understanding with industry representatives and government under which they committed to working towards a significant reduction in illegal file-sharing. Ultimately, however, the memorandum of understanding failed as rights holders and the ISPs could not agree how the costs of any measures to reduce OCI should be borne.

Consequently, the government was forced to legislate in this area and the relevant provisions were enacted in the UK Digital Economy Act 2010 ('DEA'). Throughout its passage throughout Parliament, the provisions relating to OCI caused widespread controversy and were heavily amended at each stage.

To deal with OCI, the DEA foresees two phases of regulation. The first phase consists of a mechanism pursuant to which right holders would detect the IP addresses of suspected online infringers and forward these IP addresses to the relevant ISPs. The ISPs would then send warning notices to the suspected infringers. The ISPs would also be required to provide to right holders an anonymous list of subscribers for whom the ISP had previously received a large number of infringement notices from the right holders. This anonymous list would permit right holders to go to court in order to request the name of the relevant subscribers for the purpose of bringing individual copyright infringement actions. The second phase of regulation consists of technical measures that ISPs may be required to implement in order to limit OCI. These technical measures may include the limitation of Internet access for certain subscribers, a measure similar to the French graduated response regime.

1 Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular on electronic commerce, in the Internal Market.

2 Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the Information Society.

3 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

Both phases are contingent on the adoption of detailed implementing rules by OFCOM. The DEA provides either that the detailed rules would be developed in the form of a code of conduct by industry stakeholders, a code which would then be approved by OFCOM, or in the absence of agreement by industry stakeholders, that the code would be adopted directly by OFCOM. Shortly after adoption of the DEA, OFCOM launched a public consultation regarding the draft code of practice that OFCOM intended to adopt. In the meantime, two ISPs challenged the DEA before the High Court of England[4] on the grounds that the DEA violated several European directives and also constituted a disproportionate restriction on the fundamental rights of Internet users. The High Court validated virtually all provisions of the DEA. After the High Court's decision, the two UK ISPs lodged an appeal before the Court of Appeal. On March 6, 2012, the Court of Appeal upheld the initial decision of the High Court[5]. Consequently it is now possible for OFCOM to adopt the initial code of obligations that would permit the first phase of the DEA to go into operation. OFCOM issued a new draft of these regulations on 26 June 2012 for public consultation. OFCOM proposes that the costs of the ISPs and OFCOM should be split 75:25 between the copyright owners and the ISPs. There is likely to be considerable debate over this proposal however it is not clear when this will happen. All the current government has said is that based on current plans, and subject to Parliamentary approval, the first notification letters would be sent in late 2015.

Twelve months after the initial obligations code comes into force, OFCOM must prepare a report for the Secretary of State containing a detailed assessment as to whether the initial phase consisting of the sending of notices to subscribers has resulted in a decrease in OCI. The Secretary of State can then instruct OFCOM to conduct further assessment, including industry consultation, as to whether additional technical measures should be imposed on ISPs in order to limit the OCI. OFCOM must then prepare a report for the Secretary of State assessing the effect of various technical measures. Based on that report the Secretary of State may make an order that ISPs implement those technical measures.

4 R, on the Application of British Telecommunications PLC and Another v Secretary of State for Business, Innovation and Skills and Others [2011] EWHC 1021.

5 R, on the Application of British Telecommunications PLC and Another v Secretary of State for Culture, Olympics, Media and Sport [2012] EWCA Civ 232.

However, the Secretary of State's order would first have to be approved by both Houses of Parliament.

In addition to granting the Secretary of State the power to impose technical measures on ISPs, the DEA empowers the Secretary of State to adopt regulations regarding court injunctions requiring service providers to block access to sites for the purpose of preventing OCI. The service providers that could be affected by injunctions of this type would include publishers of websites, hosting providers, and providers of other online services. This was the most controversial aspect of the OCI provisions and was heavily watered down during its passage through Parliament. In its final form, industry must be consulted and, as with the order to impose technical measures, the Secretary of State must gain approval by both Houses of Parliament within a 60 day "super-affirmative" window. The current UK government indicated in 2013 that it did not intend to use this power, in particular as s97A of the UK Copyright, Designs and Patents Act already provides copyright owners with a remedy, which has now been tested by rights holders with success[6].

There have now been several applications for website-blocking injunctions in the UK under s97A, all of which have been successful. The success of this remedy for copyright holders has even led to the first occasion on which a website-blocking order has been made in Europe in order to combat trade mark infringement[7]. In this case, the Judge analysed data submitted on the efficacy of s97A injunctions, which showed a "marked and sustained drop in traffic to targeted websites after blocking injunctions were implemented." The data also suggested that users of the blocked websites did not circumvent the block (e.g. by using VPNs) but instead used different websites. Consequently, Arnold J was persuaded of the efficacy of awarding a blocking injunction. The claimants also had to show that the relief was necessary, dissuasive, not costly or complicated, struck a "fair balance" between fundamental rights and was proportionate. Arnold J found that the relief met all these conditions.

6 Case of Twentieth Century Fox Film Corporation and Others v British Telecommunications PLC [2011] EWHC 1981 (Ch) and Dramatico Entertainment Limited and Others and British Sky Broadcasting and Others Limited [2012] EWHC 268 (Ch).

7 Cartier International AG and Others v BskyB and Others [2014] EWHC 3354 CH.

France

In 2006, France transposed into national law the InfoSoc Directive. The French law, called the "DADVSI" in French, crystallized debates regarding the appropriate measures that should be taken to limit OCI. A number of French parliamentarians argued that the individual downloading of copyrighted content for private purposes should be covered by a compulsory licence for private copying and not considered as infringement. Individual lawsuits against Internet users for file sharing in France were in some cases unsuccessful because judges balked at applying harsh infringement sanctions to teenagers who download music for personal usage. It became clear that French copyright law was ill-adapted to the problem of OCI, in part because France's penalties for copyright infringement were so severe.

Ultimately, the DADVSI did not create compulsory licencing for private downloading. Instead, the law contained a provision stating that individual peer-to-peer downloads would no longer be considered a crime under French copyright law, but would be considered only a misdemeanour subject only to a low-level fine equivalent to a parking ticket. France's Constitutional Court held that this lightened sanction regime was unconstitutional because it created two different kinds of punishment for an act of copyright infringement depending solely of the technology used to commit the infringement. The court found that this difference in sanctions violated the constitutional principle of equality of punishment for the same offence.

The DADVSI created a new regulatory authority, then called the "ARMT", to regulate questions linked to interoperability of technical protection measures. The ARMT was supposed to strike a balance between copyright and freedom of expression by ensuring that technical protection measures do not frustrate legitimate uses of the protected work, or prevent interoperability. However, the ARMT was not given any rulemaking authority. The ARMT was to intervene solely in individual cases, either as a mediator or as an arbitrator to order access to interoperability information in appropriate cases. The ARMT was inactive, in part because music labels did not end up making extensive use of anti-copy measures on CDs. The ARMT survived, however, and ultimately became the French regulatory authority today known as the "HADOPI."

Following adoption of the DADVSI, the French President urged right holders, ISPs and several large hosting platforms to sign a charter pursuant to which right holders undertook to make more content available for legal online offers, ISPs and other Internet platforms agreed to implement graduated response and to experiment with filtering, and the government agreed to put into place a legal framework that would support both the development of legal offers and the implementation of a graduated response regime. After signature of the Elysée Agreement, neither right holders nor ISPs took action, and waited for the government to take the first step by putting into place the promised new legal framework for graduated response. The government then proposed the controversial HADOPI law, which would introduce the graduated response regime in France, a regime that could ultimately lead to the temporary suspension of Internet access for repeat infringers.

The first version of the HADOPI law was adopted by both houses of French Parliament, but invalidated in part by the French Constitutional Court. The first version of the law had given the HADOPI administrative agency the power to order the suspension of Internet access for certain repeat infringers after a procedure in which the suspected infringer could present his or her defence. The Constitutional Court found that the suspension of Internet access constituted a serious restriction on freedom of expression and that such a serious measure should only be ordered by a judicial authority, and not by an administrative agency. After invalidation of this portion of the HADOPI law, the government introduced an amended version that provided for an expedited procedure pursuant to which a court would make the ultimate decision as to whether to suspend Internet access for repeat infringers. Highly debated and applied only once, these provisions were deleted by Decree n° 2013-596 of 8 July 2013, even if they remain included in other provisions of the French Intellectual Property Code.

Under the HADOPI graduated response regime, right holder organizations collect IP addresses of suspected infringers using peer-to-peer networks. The evidence is then transmitted to the HADOPI regulatory authority, who then asks the Internet access providers to provide the names of the subscribers corresponding to the IP addresses. According to HADOPI's activity report for 2013 – 2014, 12,265,004 identification requests were sent in total to the Internet access providers. Three steps are then followed by the HADOPI: In the first one, the HADOPI sends an initial e-mail to the relevant subscribers informing them of their duty to ensure that their Internet access is not used for infringing purposes, and reminding the subscriber of the existence of legal online offers. According to its activity report for 2013 – 2014, the HADOPI has sent out 3,249,481 first warnings. In the second step, repeat infringers then receive a registered letter from the HADOPI stating that the subscriber has been identified again as the source of infringing content, and that if the conduct does not cease the HADOPI may transmit the file to the public prosecutor for sanctions, which may include suspension of Internet access. According to the last figures published by the HADOPI in 2014, 333, 723 registered letters of this type have been sent. For subscribers that continue to show evidence of infringing activity, the HADOPI then selects, in the third step, the files to be reviewed and may ask the relevant subscriber to participate in a hearing. Only professionals and legal entities are now required to attend said hearing. Approximately 60 hearings took place since the beginning of the third step in June 2011. The HADOPI then hands down a decision. Since 2011, 1,289 decisions were handed down by the HADOPI. The HADOPI can send the files to the public prosecutor if the graduated response regime has not put an end to the illicit acts. Among the above mentioned 1,289 decisions handed down, only 116 decisions decided to send the file to the public prosecutor. No public data is available regarding the following court proceedings after these decisions. It appears that around 25 decisions were handed down by the courts and the amounts of the penalties ordered are between 50 and 700 euros. Only one decision ordered the suspension of the Internet access in June 2013, before its deletion in July 2013.

Since the date it was created, the HADOPI has been subject to vocal criticism, particularly from advocates of Internet freedom. A number of influential members of the French socialist party criticized the HADOPI as being a waste of money, an invasion of fundamental rights and ineffective. Since the election of the socialist François Hollande as President of France, and the new socialist majority in Parliament, the future of the HADOPI regulatory authority and of the French graduated response regime was uncertain. Several initiatives were taken to try to amend the regime. In this regard, numerous proposals, reports and recommendations were drafted, such as the

> the French socialist party criticized the HADOPI as being a waste of money, an invasion of fundamental rights and ineffective

so-called Lescure report[8] dated May 2013, the Imbert Guaretta report of May 2014[9], the 2014 annual study of the *Conseil d'Etat*[10], together with charters signed between the stakeholders. However, no amendment was enacted to date.

In the meantime and similarly to other European countries, like the UK, Article 8(3) of the InfoSoc Directive was transposed in the HADOPI law of 12 June 2009 in Article L. 336-2 of the French IP Code. However, although Article 8(3) of the InfoSoc Directive mentions *"intermediaries"*, the French article mentions *"anybody"*. In essence, Article L. 336-2 states that: *"(…) the court of first instance (…) may order any measure to prevent or cease any copyright or neighbour rights infringement, against anybody likely to contribute to remedy"*.

These provisions remained unnoticed at the beginning. However, they were applied twice to date with success. They were applied for the first time in a famous decision *"Allostreaming.com"* of the Paris Court of First Instance dated 28 November 2013, in which five French ISPs were ordered to block streaming websites. Another decision of the Paris Court of First Instance, ruling in summary proceedings and mentioning the decision of the CJEU of 27 May 2014 *"Telekabel"*, was rendered against The Pirate Bay on 4 December 2014. In this case, four French ISPs were ordered to block for France and for one year the streaming website www.thepiratebay.se, its eighteen redirection sites mentioned in the order, three mirror sites and a long list of proxies, by any efficient measure, including the blocking of the domain name.

Spain

On 31 December 2011, the Spanish Official Gazette published the Royal Decree 1889/2011, known as the "Sinde Act"[11], which first developed the functions of the Spanish Copyright Commission ("SCC") and implemented the notice and takedown procedure for the protection of copyrights on the Internet. The SCC had been originally created within the Culture Ministry as a national agency for the defence of copyrights and assigned with arbitration and mediation functions. However, its role was enhanced by the controversial anti-Internet piracy "Sinde Act", which developed a new notice and takedown procedure for the removal of copyright infringing content from the Internet, and created a new division of the SCC ("Section Two") in charge of dealing with such new procedure. The operation of this new Section Two of the SCC and the possibility of using the notice and takedown mechanism came into force on 29 February 2012.

Due to the limited success of the previous legislative effort, the Spanish Copyright Act has been recently amended by Act 21/2014 of November 4, 2014, which came into force, in general terms, on January 1, 2015. This new reform has (a) further developed the safeguarding of intellectual property rights on the Internet, (b) broadened the liability of intermediary service providers and (c) increased penalties for copyright infringement.

Act 21/2014 establishes a time limit of one year for the Government to ready the preparatory works for a comprehensive reform of the Intellectual Property Act,

> The new reform of the Spanish Copyright Act has broadened the liability of ISSPs ad increased penalties for copyright infringment.

8 http://www.culturecommunication.gouv.fr/var/culture/storage/culture_mag/rapport_lescure/index.htm.

9 http://www.culturecommunication.gouv.fr/Ressources/Rapports/Outils-operationnels-de-prevention-et-de-lutte-contre-la-contrefacon-en-ligne.

10 http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Etude-annuelle-2014-Le-numerique-et-les-droits-fondamentaux.

11 This refers to certain provisions of the Sustainable Economy Act 2/2011, of 4 March 2011 which deals with copyright infringement and are known as "Sinde Act" after the former Spanish Minister of Culture Ms Ángeles González-Sinde who supported such provisions.

and serves as a short-term solution to the most urgent challenges, among which the fight against online piracy is included. In this sense, it introduces the following measures (which entered into force on 5 January 2015):

a) The safeguarding of intellectual property rights on the Internet

Although the "Sinde Act" had implemented the notice and takedown procedure for the protection of copyrights on the Internet, this amendment to the Spanish Copyright Act shows a considerable improvement in the procedure. As a result, the Section Two of the SCC (in charge of the notice and takedown procedure) has been empowered with more effective reaction mechanisms, it has a broader scope of application and it introduces some technical improvements.

The safeguarding procedure is applicable against (i) alleged copyright infringing activities by information society service providers ("ISSPs") (e.g. blogs, websites, etc.), as long as the service provider has a significant audience in Spain, or if there is a significant volume of non-authorized works displayed on the website, and (ii) ISSPs providing the description and location of presumably infringing works by means of an active contribution (not mere technical intermediation), such as web pages providing structured and classified links to infringing works. Note that the SCC does not act against individuals downloading content, but only against ISSPs.

One of the main innovations brought by the reform is the possibility of initiating the procedure "ex-officio" (i.e. directly by the SCC), with just a previous complaint from the holder of the rights allegedly infringed. Previously, the rights holder had to file a formal request which was much more complex. Now, the complaint from the right holder is only subject to the previous requirement of having requested removal to the ISSP unsuccessfully. Also, it is now possible to make a generic request for removal instead of reporting the infringements one by one.

b) Liability of intermediary service providers

When the SSC issues a resolution confirming copyright infringement, ISSPs may be required to remove infringing content. If the ISSP refuses to collaborate, intermediary service providers (i.e. advertising, electronic payment providers, etc.) may be required by the Copyright Commission to suspend the corresponding service they offer to the ISSP. This includes access providers, which can be ordered to block access to infringing websites aimed at the Spanish territory. Note that, in order to request a suspension of the service or blocking of access, the Copyright Commission has to be previously authorized by a judge.

In this context, under the amended Spanish Copyright Act, the lack of cooperation with the Copyright Commission (i.e. not suspending the service) is regarded as a very serious infringement of the Information Society Services and E-Commerce Act 34/2002, of July 11, 2002, sanctioned with fines from €150,001 to €600,000.

In addition, in cases of serious infringements, or where the social impact of the infringement is high, the ISSP can be requested to cease activities for a maximum period of one year. In order to ensure the effectiveness of this measure, intermediary service providers may be requested (if approved by a judge) to suspend the service provided to the ISSP. Here again, the lack of cooperation (i.e. not suspending the service) is regarded as a very serious infringement of the Information Society Services and E-Commerce Act 34/2002, of July 11, 2002, sanctioned with fines from €150,001 to €600,000.

Strictly speaking, these two infringements are really one and the same (both sanction the lack of cooperation of the intermediary service provider), but can be triggered by the two different situations described above.

c) Penalties for copyright infringement

In addition to the penalties for intermediary service providers described above, the amendment provides for increased fines for those ISSPs who do not comply for two or more times with requests for removal. This conduct is regarded as a very serious infringement sanctioned with fines from €150,001 to €600,000. Same penalties are envisaged for the resumption of infringing activities by the same ISSP for two or more times.

Finally, as previously stated in (b), in cases of serious infringements, or where the social impact of the infringement is high, the infringement can lead to the following consequences: (i) the publication of the resolution in the Spanish Official Gazette and in two national newspapers or on the ISSPs website, and (ii) the

ISSP can be requested to cease activities for a maximum period of one year.

As a final note, it must be said that even though these measures have already had an impact[12], a regulation developing Act 21/2014 is still pending to be issued by the Government. Thus, the end results and effectiveness of these new measures may still increase in the near future.

Germany

The German legislator did not see a need to insert special provisions into German law to implement Article 8(3) and recital 59 of the InfoSoc Directive as it was of the opinion that the possibility for right holders to apply for an injunction against an intermediary was already provided for under the German Copyright Act and Telemedia Act. Further, unlike the UK, France and Spain, no laws have been or are planned to be introduced in Germany obliging ISPs to assist rights holders in the reduction of OCI.

Germany relies on a system to fight OCI in which at first warning letters, including pre-formulated cease-and-desist undertakings, are sent to copyright infringers. These warning letters are a well-known measure in the general populace and already stop a majority of private OCI cases in Germany. If the infringers do not sign the undertaking the rights holders have as a second step the possibility of filing for a preliminary injunction against the infringer to stop the infringing act.

Further Germany has extensive case law concerning the so-called "Störerhaftung" (Breach of Duty of Care) according to which not only the copyright infringer himself can be held liable but also auxiliary persons to the perpetrator of the copyright infringement. The duty of such an auxiliary person is limited to cease and desist and removal. The "Breach of Duty of Care" has three main requirements:

1. The auxiliary person must in some way contribute willingly and causatively to the copyright infringement, e.g. by providing the means of access to websites with pirated content.
2. The auxiliary person must have had the possibility of preventing the copyright infringement.
3. The auxiliary person must also have violated due diligence obligations. This third requirement serves

12 As an example, among others which have followed after, Spain's very famous download site "Series.ly" reacted to the new legislation by removing all content that might infringe copyright law days before its entry into force.

as a kind of corrective to prevent the breach of Duty of Care liability from becoming excessive. It is used to incorporate a balancing of interests between the auxiliary person and the rights owners. Generally it is required that the auxiliary person is or should have been aware of the copyright infringement either because the infringement is apparent and easily recognisable in itself or because the auxiliary person has been made aware of the infringement.

Whether these existing German rules really are sufficient to implement the relevant provisions of the InfoSoc Directive is still disputed amongst scholars. In two recent cases, German courts refused to grant an injunction against an access provider based on the existing provisions.

The decision of the Higher Regional Court of Hamburg of 21 November 2013 (U 68/10) concerned a claim of the Society for Musical Performance and Mechanical Reproduction Rights (GEMA) against the biggest German access provider. The defendant offered access to a website where users could access pirated copyright protected works. Although the court recognized the copyright infringement and the general possibility of liability of access providers it dismissed the claim as it deemed the requested blocking measures to be unreasonable. The Court stated that the access provider's business model was "neutral concerning the content, socially adequate and in accordance with the law". Further, the blockage could inherently lead to the restriction of access to works which are not protected or not pirated which would result in the potential infringement of third parties' rights. Lastly the Court claimed that the blocking measures would cause the access provider to violate the confidentiality of telecommunications that is protected under Art. 10 of the German constitution as it could be necessary to use protected information regarding the communication process to achieve the blocking.

This reasoning was followed by the Higher Regional Court of Cologne in its decision of 18 July 2014 (6 U 192/11) in a claim against a music file sharing platform. This decision was made after the Telekabel decision of the CJEU. The German Court extensively referred to the Telekabel decision. They concluded from that decision that there is generally the possibility of granting a blocking order in Germany. After clarifying that this general possibility exists in Germany the Court continued to examine extensively whether a blocking order was necessary and acceptable in this particular case. The Court weighed up the rights of the applicant and defendant in a similar way as the Higher Regional Court of Hamburg and decided in favour of the defendant arguing that an injunction granting the blocking of access to a website would be unreasonable for the access provider.

Both decisions are pending before the German Federal Supreme Court.

As the second decision was based on the Telekabel case of the CJEU the German Federal Supreme Court will most likely not overturn the decision on the basis of the principles in that case. It might however be that the German Federal Supreme Court weighs the interests of applicant and defendant differently and therefore reaches a different conclusion. Most likely the German Federal Supreme Court will set high barriers for website-blocking injunctions in Germany in these appeal decisions.

Rest of the World

Outside Europe there have also been significant developments in Asia, notably Australia, where the government has announced new initiatives including amendments to the Australian Copyright Act that will enable rights holders to apply for an injunction requiring ISPs to block websites operated outside of Australia. In Russia, the government has introduced amendments to its anti-piracy law which will come into force on 1 May 2015, extending the regime. At the same time, the Russian government is considering a proposal by the Russian Union of Rightsholders to introduce a fixed royalty fee to be paid by telecom operators to rights holders.

Australia

The Australian government announced in December[13] new initiatives to address concerns about online copyright infringement. A 'frequently asked questions' (FAQ) document[14] about the reforms was also released. There were two key planks to the announcement:

a) a call to industry to develop a new industry code within 120 days, or face new binding regulatory arrangements to address online piracy; and

b) amendments to the Copyright Act 1968 (Copyright Act) will be made to enable rights holders to apply for a court order requiring ISPs to block access to websites

13 http://www.attorneygeneral.gov.au/Mediareleases/Pages/2014/FourthQuarter/10December2014-Collaborationtotackleonlinecopyrightinfringementaspx.

14 http://www.malcolmturnbull.com.au/issues/new-measures-to-tackle-online-copyright-infringement.

operated outside of Australia which provide access to infringing content.

The new measures will be reviewed after 18 months to assess their operation and effect.

The Australian Communications Alliance published a draft code on 20 February 2015[15]. This draft code is currently in a 30-day public consultation phase before it is finalised and put before the Australian Communications and Media Authority. The consultation phase is required by the Telecommunications Act 1997, but should also assist in addressing criticisms of previous code processes about the level of consumer involvement. The draft code is not yet complete, and is subject to change after this consultation period has ended. One of the key issues for determination – the costs of implementing the code, and who should bear those costs – is still under negotiation and the draft code is currently silent on the issue of costs.

Once finalised, the code will be registered as an industry code under Part 6 of the Telecommunications Act. Compliance with the code will be one of the issues to be assessed by a Court in determining whether an ISP should be held liable for 'authorising' any infringements committed by customers under ss. 36 or 101 of the Copyright Act.

The Government set out its expectations and policy objectives for the code in a letter to industry[16]. The draft code complies with these expectations and objectives by creating a copyright notice scheme. This scheme will allow rights holders to notify ISPs of any infringements of copyright by submitting a report in a standard form to the ISPs, which will identify the IP addresses of suspected online infringers. ISPs will then send a notice to the holders of the account to which that IP address had been allocated at the time of the infringement. In the first instance ISPs will send a notice containing educational material explaining where to access legitimate alternatives and how to avoid copyright infringement online. A second offence will incur a warning notice and a third a final notice. The draft code allows rights holders to request a list of IP addresses that have been sent each of these notices. At this point the rights holders can apply to a federal court or tribunal for an order allowing them to obtain the identity of the holder of any account that has received a final notice from the ISP. It is crucial that until such an order has been obtained, rights holders will not have access to the identities of any alleged infringers. Final notices can be challenged by account holders, and all challenges will be passed to an adjudication panel, which has an obligation under Article 3.10.13 of the draft code not to disclose the identity of any account holder. The $25 fee for seeking an adjudication has been referred to by the Australian Communications Consumers Action Network (ACCAN) as a "fine by stealth"[17].

The draft code also provides for oversight of this procedure by allowing for the creation of a Copyright Infringement Panel ("CIP"), consisting of representatives of rights holders, ISPs and the consumer group ACCAN. The CIP will oversee the scheme by authorising the processes by which rights holders will identify infringements of copyright and overseeing the adjudication panel. The CIP will also draft all the relevant documentation such as the notices and material advertising the scheme to the public.

The legislation to implement the new site blocking measures has not yet been released. As such, the precise scope of the measures is not yet known. We do know that site blocking will only apply to overseas websites, as rights holders are not prevented from taking direct infringement action against websites operated within Australia. In considering whether to make a blocking injunction, a court would be required to have regard to the rights of any person likely to be affected by the grant of an injunction, and court rules would operate to allow the court to make any directions it considered appropriate in the circumstances.

In the original Discussion Paper foreshadowing the reforms released in July, the site blocking proposal was limited to sites where the "dominant purpose" of the website was to infringe copyright. Further, it was stated that rights holders would be required to meet any reasonable costs associated with an ISP giving an effect to an order and to indemnify the ISP against any damages claimed by a third party.

In contrast, the December Government announcement refers to site blocking of a website "which provides access to infringing content," and makes no mention of ISP costs or indemnities. It is unclear whether this represents a shift in policy or whether the legislation to be introduced will more closely reflect the July proposal.

15 http://www.commsalliance.com.au/__data/assets/pdf_file/0005/47570/DR-C653-2015.pdf.

16 http://www.attorneygeneral.gov.au/Mediareleases/Documents/LettertoIndustryLeaders.pdf

17 http://accan.org.au/news-items/media-releases/1019-copyright-notice-scheme-must-respect-consumer-protections.

Russia

On 24 November 2014, the Russian President signed into law a bill introducing amendments to the so-called Anti-piracy Law[18] and expanding its scope to all types of copyright-protected content available on the Internet, except for photographs (the "Law")[19]. The Law will take effect on 1 May 2015.

Under the Law the following procedure will become available for rights holders wishing to restrict access to audio-visual works which have been placed on the Internet illegally:

The right holder may seek a preliminary injunction before the Moscow City Court against illegal use of content on a particular websites.

Once a preliminary injunction has been obtained, the right holder may file an application with the Russian state authority in charge – Roskomnadzor[20] – seeking restriction of access to the website. Within three business days Roskomnadzor must determine the hosting provider and send an electronic notification requesting the removal of the infringing content;

Within one business day from the date of receipt of notification, the hosting provider must inform the website owner of the need to immediately remove the infringing content from the website or restrict access to such content. The website owner has one business day to remove the infringing content.

If the website owner fails to do so, the hosting provider must restrict access to website within three business days from the date of receipt of Roskomnadzor's notifications. If the website owner and/or the hosting provider fail to restrict access to the website, Roskomnadzor sends the information on such website to telecom operators, which must restrict access to the website within twenty-four hours.

In addition to the above procedure, the Law allows the right holder to undertake an out-of-court measure by sending a complaint to the website owner. Within 24 hours from the complaint's receipt the website owner must cease the infringement or present proof evidencing the lawful use of content on the website. To make this work the Law obliges the website owners to disclose his/her/its name, address and email on the website.

The Law further provides for a possibility of perpetual restriction of access to the website where infringing content was placed repeatedly and this has been confirmed by the court's ruling. Upon such court's ruling Roskomnadzor sends the information on such website to telecom operators which in turn must restrict access to the website within twenty-four hours upon receipt of the Roskomnadzor's notification.

In parallel with the discussion on the amendments to the Law the Russian Union of Right Holders (the "RUR") has proposed fighting piracy by introducing a fixed royalty fee to be paid by the telecom operators to right holders in exchange for unlimited use of almost all types of content on Internet. It is suggested the royalty will be collected by a collecting society accredited by the state. This initiative is now under consideration by the Russian Government.

These two parallel processes (one – introduction of a thorough anti-piracy legislation; and another – introduction of a fixed royalty fee for unlimited use of content on Internet) clearly do not look like a perfect match.

Conclusion

Is 2015 the year of the website-blocking injunction? The ability for rights holders to apply for website-blocking injunctions against ISPs certainly appears to be a feature of all the new regimes adopted by governments seeking

"the Russian Union of Right Holders (the "RUR") has proposed fighting piracy by introducing a fixed royalty fee to be paid by the telecom operators"

18 Federal Law No. 187-FZ dated 2 July 2013 "On amending certain legislative acts of the Russian Federation on protection intellectual rights in information-telecommunication networks" (the "Anti-piracy Law").

19 Federal Law No. 364-FZ dated 24 November 2014 "On introduction of amendments to Federal law "On information, information technologies and the protection of information" and to the Russian Civil Code" is available at (in Russian): http://www.rg.ru/2014/11/27/gpk-dok.html.

20 Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications.

to reduce OCI in various countries around the world. Following the CJEU ruling in *Telekabel* and the spate of successful applications in the UK over recent times, it seems likely that we will see an increase in the number of websites making available infringing content being blocked both within Europe and elsewhere. This is good news for rights holders although there are concerns that users can easily circumvent certain blocking measures, using VPNs or other methods, particularly if the website is not blocked in every jurisdiction worldwide. Nevertheless, it is encouraging for rights holders that governments are also improving national graduated response regimes for reducing OCI across the globe.

Penelope Thornton
Senior Associate, London
T +44 207 296 5665
penelope.thornton@hoganlovells.com

Eva Vonau
Associate, Hamburg
T +49 40 41993 560
eva.vonau@hoganlovells.com

Camille Pecnard
Senior Associate, Paris
T +33 1 5367 2362
camille.pecnard@hoganlovells.com

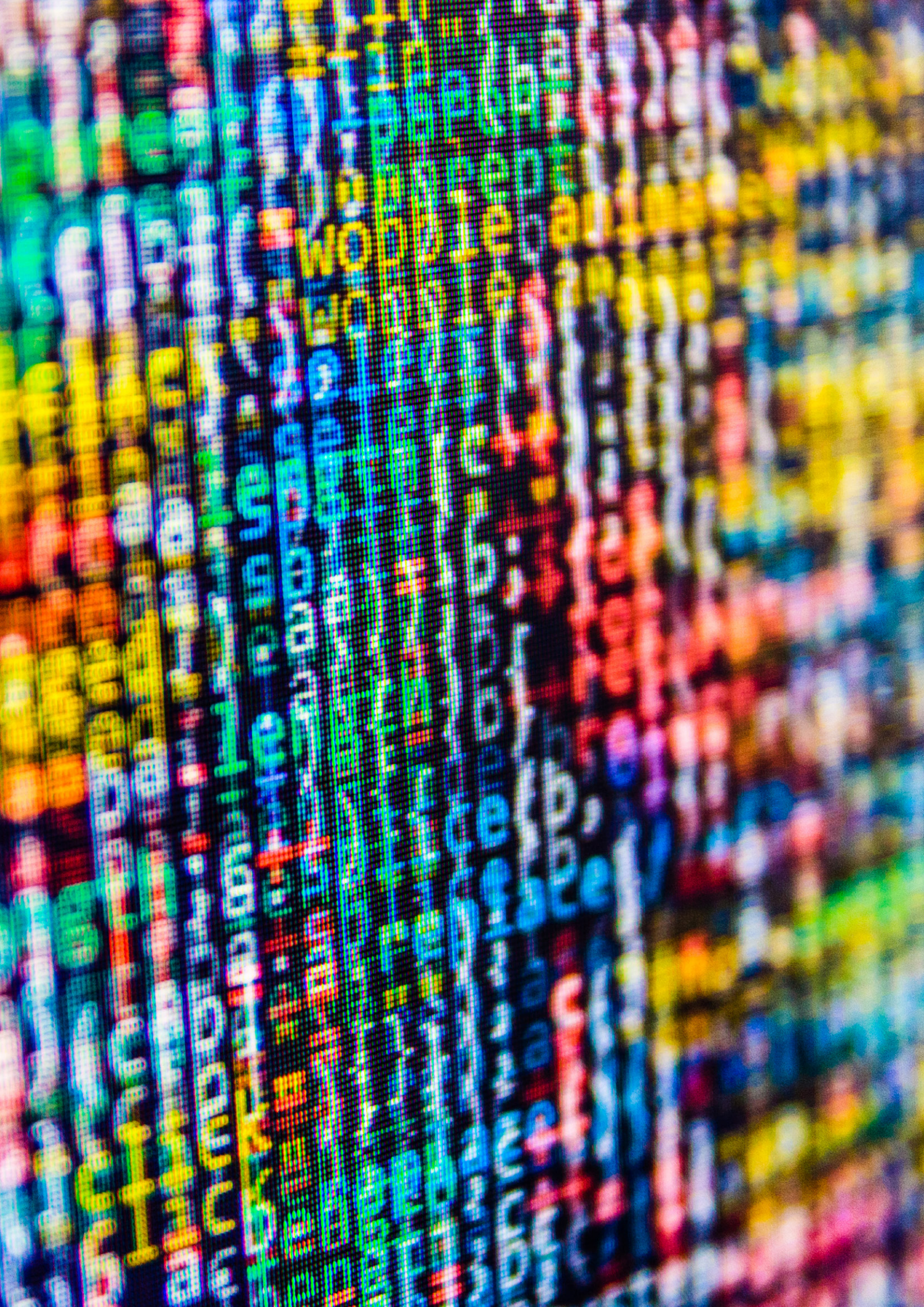
Carolyn Dalton
Executive Director, Policy Australia Pty Ltd
T +61 402 791 031
info@policyaustralia.com.au

César Ortiz-Úrculo
Associate, Madrid
T +34 91 349 8160
cesar.ortiz-urculo@hoganlovells.com

Natalia Gulyaeva
Partner, Moscow
T +7 495 933302 5289
natalia.gulyaeva@hoganlovells.com

Laur Badin
Junior Associate, Madrid
T +34 91 349 8186
laur.badin@hoganlovells.com

Maria Sedykh
Associate, Moscow
T +7 495 933300 0235
maria.sedykh@hoganlovells.com



Net Neutrality – A Global Debate

The net neutrality debate has run to fever pitch in the United States, with the Federal Communications Commission (the "FCC") issuing controversial new rules that will treat Internet access like a public utility. President Obama personally weighed in on the issue, leading critics to accuse the FCC of insufficient independence from the White House.

The headlines have made the most of the debate in the United States, but it is clear that regulators across the globe are grappling with the same issues as internet traffic volumes soar and traditional revenue models in telecommunications and content distribution face disruption by new technologies and services.

On March 4, 2015, the European Council of Ministers reached agreement on net neutrality language to be inserted in a future European regulation. The Council's language stops far short of the strict net neutrality language supported by the European Parliament, which will lead to tense negotiations between the EU institutions in the coming months. Meanwhile, one national regulator in Europe has already started to issue sanctions for net neutrality violations.

In Asia, the debate has yet to emerge in full force, but the flashpoints are coming with increased frequency across the region. Most recently, in December Indian mobile service provider Airtel announced plans to surcharge users of popular voice over internet (VoIP) services such as Skype, Whatsapp and Viber. Airtel faced a firestorm of public criticism over the move, but its hasty retreat from these plans was put down to confirmation of plans by the Telecom Regulatory Authority of India to launch a consultation on net neutrality issues rather than any buckling to consumer pressure.

It is clear that net neutrality is now an issue with global dimensions that will continue to make the headlines through 2015.

Net Neutrality Defined

"Net neutrality" is simple in its conception – the idea that internet service providers should enable internet access to all content and services without discrimination.

Proponents and opponents of formal rules enshrining net neutrality into law are often in agreement as to desired outcomes (at least at a superficial level) but at the same time in fundamental disagreement as to the means.

Large internet service providers will point to the practical necessity of managing finite network capacity in order to ensure quality service for all – for example, by "throttling" users of high volume services, such as those who use the internet to stream feature length films. They also point to a need for flexibility in terms of how they deal with content providers and users. Commercial deals giving faster access speeds to high volume content providers and differentiated service packages to high volume users will support higher investment levels in new networks, creating additional capacity for all.

These assertions, argue net neutrality supporters, point up some critical areas for concern. If internet service providers are permitted to create these "internet fast lanes", network capacity will effectively be sold off to the highest bidder, with smaller content providers and consumers having more limited financial resources unable to enjoy the benefits promised by an open internet. Heavier regulation, directed at constraining or eliminating operators' discretion to prioritise, is therefore needed.

Net Neutrality – A look at market context

Viewing the net neutrality debate from a global perspective gives insight to the particular problems that inform the debate, and, we would argue, the most appropriate regulatory solutions.

In the U.S., fixed-line broadband competition is generally limited to competition between the local cable network and the local telecom network. This relative lack of competition in the fixed line broadband market has made net neutrality advocates particularly nervous about discriminatory practices, and the case for regulation easier. Competition in mobile broadband in the U.S. seems more robust, which explains why the FCC has until now applied lighter net neutrality rules to mobile operators.

The FCC's approach to mobile operators changed with its February 26 order, which treats mobile and fixed-line operators the same, while recognizing the capacity constraints that apply to mobile services. The other remarkable aspect of the FCC's order is that it classifies broadband access as a "telecommunications service," which gives the FCC clearer statutory footing to regulate the service. Critics worry that the FCC will use this new authority to over-regulate, including imposing

retail price constraints. The FCC so far proposes to use its new authority with restraint, imposing only a few minimal regulatory obligations, including the principle of non-discrimination. The non-discrimination principle is by far the most controversial, because it would prohibit many kinds of commercial agreements between ISPs and content providers. The FCC also said that it would intervene in interconnection and peering disputes, if there were evidence of "unreasonable" practices.

Europe's regulatory framework has emphasized intra-modal competition, based largely on local loop unbundling. Many European households have a choice among three or more fixed-line broadband providers. Europe's approach to net neutrality has emphasized transparency and competition: if consumers are unhappy with how a broadband provider deals with content, the consumer can switch providers. However two countries in Europe (The Netherlands and Slovenia) enacted stricter net neutrality rules, leading to a divergence in how EU Member States regulate net neutrality. This prompted the European Commission to propose more detailed net neutrality rules in a proposed regulation. The proposed regulation has brought to the surface differing policy approaches: the European Parliament wants to circumscribe the use of "managed" or "specialized" services by ISPs, whereas the European Council of Ministers wants to give ISPs freedom to innovate, as long as basic Internet access is not impaired. Meanwhile, the Netherlands has used its net neutrality law to sanction telecom operators who provide special retail offers that include content conditions. One practice is "zero rating," which consists of giving subscribers unlimited access to certain content without that content being counted for purposes of data limits. It is unclear how the new EU legislation, which is likely to be adopted in late 2015, will deal with "zero rating." The proposed EU text is also silent on paid peering, which remains a sensitive issue for certain content providers.

Asia has a number of markets – Japan, Hong Kong, Singapore and South Korea, in particular – that are often characterised as "broadband paradises" in the sense that internet access has a high quality and a low price. It is noteworthy, however, that the governments in these jurisdictions have all studied net neutrality issues in recent years. While all concluded that continued vigilance is necessary, for the most part regulators determined that existing anti-trust laws and consumer protection laws satisfactorily meet all realistic net neutrality concerns.

Japan is an apt case study for Asia. Liberalisation of internet access markets began there in the 1980s. When NTT, the incumbent domestic carrier, was split and privatised it was required to open up its facilities to competitive DSL services on fairly generous terms. The government helped finance to new market entrants and by 2001, Japan had the highest number of DSL subscribers anywhere in the world.

Effective retail competition for broadband is a common characteristic of these advanced Asian markets. Asia's high population densities also no doubt help de-risk plans for network investment. These characteristics are critical differentiators to the United States market context.

This is not to say, however, that net neutrality concerns are not emerging in Asia. Incumbent telecoms operators have clashed with regulators in Singapore, South Korea and now India over plans to surcharge users for the use of VoIP, services that use significant bandwidth and, of course, erode operators' telephony margins. We expect the debate to continue to develop across Asia as bandwidth-hungry services, increased use of mobile and the emergence of next generation networks continue to come to the fore.

Conclusion

The need for net neutrality regulation depends on local context, including the level of broadband competition, and how competition and consumer protection law is applied on the ground. In many situations, existing law provides an adequate remedy for potential abuses. In other cases, a regulatory authority needs to be specifically empowered to take action to limit discriminatory practices. The FCC and European approaches are now in alignment insofar as both regimes are technologically neutral, applying to both fixed and mobile communications. Both regimes also rely on the premise that Internet access is a service that can be regulated by telecom regulatory authorities, although the level of regulation should be limited so as not to impede innovation. A number of Asian countries that have published their analyses of net neutrality issues have arrived at broadly the same conclusions, but only recently has there been any real call to put these principles to the test.

With the publication of the FCC's new rules and the rising debate amongst the EU institutions it is clear that 2015 will see net neutrality in the headlines at a frequency never before seen, with global implications.

Winston Maxwell
Partner, Paris
T +33 1 5367 4847
winston.maxwell@hoganlovells.com

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Michele Farquhar
Partner, Washington D.C.,
T +1 202 637 5663
michele.farquhar@hoganlovells.com

Net Neutrality and implications for the connected-TV space

This article focuses on the parallels between the net neutrality debate in Internet policy, issues around carriage agreements in the pay-TV market, and implications for the nascent connected-TV space.

The meaning of 'net neutrality' is becoming a matter for debate

Traditionally, net neutrality was seen mainly as a technical issue that has implications for free speech and innovation. In particular, much of the debate and regulatory activity has centred on the 'traffic management' practices of Internet service providers (ISPs). In this context, net neutrality refers to the guarantee that Internet traffic of similar content from different sources will be treated equally. This definition of net neutrality recognises that there are legitimate grounds for traffic management based on objective reasons (for example, all voice-over-IP traffic may be treated the same irrespective of the source, but may be treated differently from email traffic), while seeking to ensure that any content provider can access any Internet user without being discriminated against.

This somewhat 'technological' definition is increasingly being challenged by business reality. In recent months, for example, Internet content providers, such as Netflix, have entered into highly publicised deals in which they pay specific ISPs to provide sufficient interconnection bandwidth to ensure the smooth distribution of video content to end users. Compared to a situation in which bandwidth is unsatisfactory, this is advantageous for ISPs because they receive a payment, but it is also valuable for content providers, because they are better able to deliver a good quality of experience for end users, thus helping stimulate demand and consumption of services. However, not everybody is happy – while everybody agrees that this falls outside the usual definition of net neutrality (because it relates to interconnection capacity rather than traffic management), Netflix and other stakeholders have argued that this is a technicality, because the effect is the same: ISPs have been able to charge content providers in return for ensuring that their customers' quality-of-experience is not degraded.

ISPs have argued that these payments are only fair in view of the need to invest in network capacity to carry the traffic in question. However, some parties, including Netflix, have argued that ultimately these deals reflect ISPs' ability to levy a "toll" for access to their customers, which may be significant and independent of any costs. They claim that ISPs have a privileged 'gatekeeper' relationship with consumers, and should be prevented from monetising this relationship by charging content providers. Instead, they argue, ISPs should use the revenue they receive from consumers to ensure that the necessary network capacity is in place. This line of argument appears to suggest that net neutrality should extend to the commercial relationships between content providers and ISPs, and not just neutral treatment of traffic, specifically by banning ISPs from charging content providers, at least in some cases.

Carriage in linear TV is not 'neutral' – but it is highly regulated

It is interesting to draw parallels between 'net neutrality' in the Internet context, and content and network relationships in the context of linear TV services.

Over the years, content providers and broadcasters have embraced multiple TV distribution platforms (terrestrial, satellite, cable, IPTV) to reach potential consumers with their linear TV offers. Commercial linear TV distribution agreements encompass a very wide variety of models, most of which are in no way 'neutral' – absent regulation aside, they generally involve a balance between the value that platform operators place on having specific TV content on their platform, the value that broadcasters place on being able to reach the platform's subscribers, and the costs associated with the infrastructure required (for example, network bandwidth, electronic programme guide (EPG) software, etc).

Carriage fees (paid by content providers to network operators) or retransmission fees (paid by pay-TV operators to content providers) often are not only a matter of market forces – they are also influenced by 'must carry' and 'must offer' obligations, as well as other laws and regulation that determine or influence what either side can charge the other. In many cases, this combination of market value and regulation has led to 'settlement-free' carriage, but in recent years there has been pressure to increase retransmission fees paid by pay-TV operators to broadcasters on both sides of the Atlantic (in the USA and selected European countries) as well as to eliminate the regulated 'technical platform' charges that broadcasters pay platform operators (for example, in Germany and the UK).

Net neutrality and traditional TV carriage models are relevant to connected TV

Similar situations and debates are beginning to arise in multiple areas of the connected-TV value chain, where many new deals are being struck to support the fast pace of innovation in connected TV.

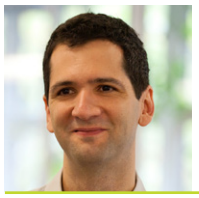
For regulators and policymakers, this raises some important questions relating to economic models, the impact on consumers, and policy objectives. For example, if connected-TV platforms can charge content providers unlimited fees in return for including their 'apps' in their devices, this might affect content providers' margins – for content providers that have a duty to commission and pre-finance audio-visual content (for example, the public service broadcasters in the EU), this might translate into reduced funding for producing original content. Conversely, if content providers can charge platforms, this may reduce innovation incentives for the latter. Consumers may also be affected – if commercial disagreements lead to key content being unavailable on some platforms, consumer choice (and, potentially, media plurality) is reduced. If 'blackouts' result from disagreements about content (rather than commercial factors), then this would raise concerns about freedom of expression.

These issues call for careful study by regulators and policy makers, to ensure that the objectives of audio-visual policy remain achievable in a converged environment. (In the EU, these objectives include: sustainable investment in, and pre-financing of, original content; supporting cultural and linguistic policies; and protecting vulnerable people from harmful content.)

The traditionally separate policy debates are becoming increasingly interlinked

Several policy issues cut across these three contexts (Internet access, pay TV and connected TV), including content producers' access to consumers; consumers' access to content; content prominence; media plurality; the bargaining power of platforms compared with content providers; and investment in content, networks and platform innovation. These issues touch on the traditionally separate policy areas of Internet, telecoms, media policy and industrial policy, and involve questions of economics, technology and culture. And increasingly, they are all interlinked.

David Abecassis
Principal, Analysys Mason
T +44 20 7395 9000
david.abecassis@analysysmason.com



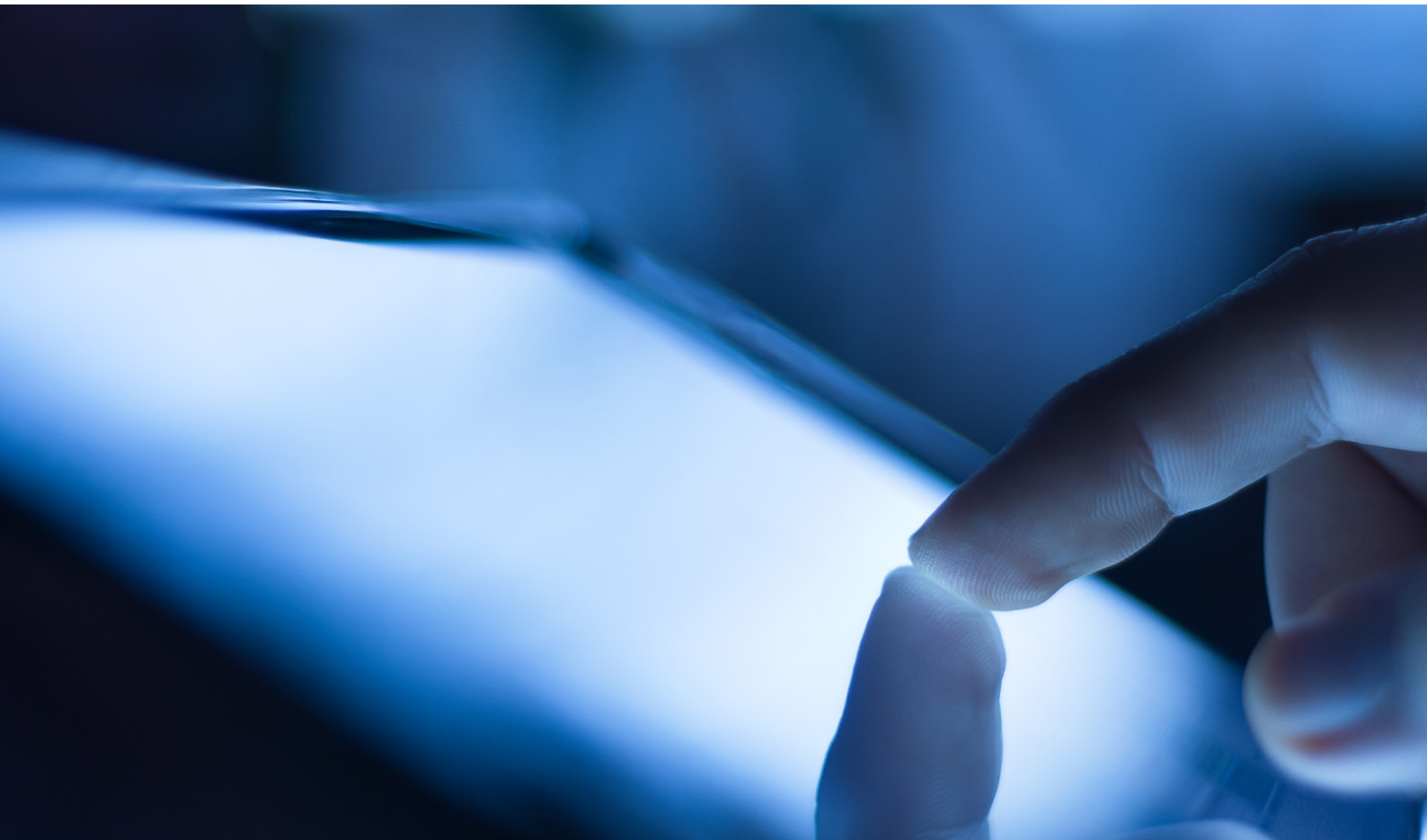
Nico Flores
Manager, Analysys Mason
T +44 20 7395 9000
nico.flores@analysysmason.com

USA and Europe: Standard Essential Patents and Antitrust

Standard essential patents (SEPs) are patents that are necessary (or have been declared essential) to a particular technology that is standardized to promote interoperability between devices or networks. Some standard setting efforts, such as the standards that enable wireless communications and Wi-Fi networking, involve hundreds or even thousands of such patents. Standards that incorporate patented technologies are the backbone of rapidly expanding worldwide markets in the information and communications technology (ICT) sector, which have nearly tripled in size since 2009. This has led to a proliferation of SEPs in the standards that are crucial to the ICT sector, such as wireless communication protocols like Long Term Evolution (LTE).

Creating a standard usually requires the standard setting organization (SSO) to choose among competing technologies. Once the standard is set, the industry may be locked into that method of doing things for an extended period of time, particularly if the industry exhibits significant network effects (i.e., every user is better off if more other users are on the same network or use a compatible device) and path dependency (i.e., each generation of the technology builds on the previous one). Therefore, when an SSO incorporates a patented technology into a standard, the patent may suddenly gain significant market power that did not exist before the standard was created. Patent holders can exploit this market power by acting opportunistically to charge the locked-in licensees more than they would have been willing to pay for the technology before the standard was set. Such exploitation by patent holders is known as "patent hold-up." Hold-up can be exacerbated when the patent holder has the right to seek an injunction against the putative infringer, which would prevent the latter from selling any of its products that may infringe on the patent holder's SEPs.

The threat of anticompetitive holdup and market power exploitation has led competition authorities to apply antitrust laws to abusive conduct related to SEPs. Antitrust investigations related to the abuse of SEPs have been percolating in the United States and Europe for the past several years, with an emphasis



on the conditions under which it is appropriate for SEP holders to seek injunctions against putative infringers. Both of the US federal antitrust enforcement agencies have signaled their intent to remain actively involved in regulating how companies acquire and enforce SEPs, the US courts have issued numerous decisions that constrain SEP enforcement and establish a methodology for determining the appropriate royalty rate for SEPs, and the EU courts and European Commission have also been active in this area. The precise antitrust boundaries regarding SEPs are still not clearly defined, and as new rules are drawn, consensus is still far away. This article discusses some of the recent high profile antitrust investigations and cases related to SEPs in the US and Europe, addressing how their outcomes could affect future business practices and antitrust investigations in a burgeoning area of commerce.

SEPs and Antitrust in the US

Recently, SEPs have been the subject of a number of significant smartphone patent lawsuits in the US, most notably involving Samsung, Apple, Ericsson, and Motorola Mobility. SEPs are also squarely within the cross-hairs of both the US Department of Justice Antitrust Division (DOJ) and the Federal Trade Commission (FTC). SEPs can trigger antitrust issues because the SEP holder can hurt competition if it does not fairly license its patent. The antitrust agencies have weighed in on the responsibilities of SEP holders (as well as SSOs) to ensure that SEPs are available on reasonable and non-discriminatory (RAND) terms to all viable licensees.

Over the last few years, the FTC entered consent orders against Robert Bosch GmbH[21] and Google, Inc.[22] pursuant to its authority under Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." The challenged behavior in both investigations related to the patent holder seeking injunctive relief based on alleged infringement of patents that had been declared essential to an industry standard requiring such patents to be licensed on fair, reasonable and non-discriminatory (FRAND) terms. The FTC did not challenge the validity of the patents, nor did it allege fraud when the standard was set. Rather, the FTC challenged the mere act of seeking injunctive relief after committing the patents to an industry standard – conduct that usually is entirely within the scope of the patent.

The consent order against Bosch required it to commit that it would (1) drop the pending SEP suits that had been brought by an entity it was seeking to acquire, and (2) not pursue any further actions for injunctive relief based on the SEPs it acquired. Google agreed to a similar commitment to close a conduct investigation related to the use of injunctions and exclusion orders in cases involving SEPs held by its then-subsidiary Motorola Mobility Inc. The FTC stated that when a company breaches a commitment to license SEPs on FRAND terms, it risks "substantial harm" to competition.

The US courts have simultaneously acted to reduce SEP holders' ability to use the threat of injunction to achieve anticompetitive hold-up. In *eBay, Inc. v. MercExchange, LLC*,[23] the US Supreme Court rejected a rule that an injunction generally will issue on a finding of infringement because monetary damages are usually sufficient to compensate for any harm from the infringement. In *Apple Inc. v. Motorola, Inc.*,[24] the Federal Circuit recently applied the same logic to FRAND-encumbered SEPs, concluding that *eBay* "provides ample strength and flexibility for addressing the unique aspects of FRAND committed patents.[25]" The court affirmed the denial of injunctive relief because the patent holder's FRAND commitments "strongly suggest that money damages are adequate to fully compensate for any infringement."[26] However, the court also held open the possibility that injunctions "may be justified where an infringer unilaterally refuses a FRAND royalty or unreasonably delays negotiations to the same effect."[27]

DOJ has also engaged in advocacy to encourage SSOs to address potential hold-up and other problems ex ante by modifying and clarifying their intellectual property rights (IPR) policies. For example, DOJ wants SSOs to limit the right of SEP holders to seek injunctions, including by constraining the right to seek an injunction to situations where the potential licensee is "unwilling" to take a FRAND license. Similarly, DOJ encouraged

21 In the Matter of Robert Bosch gmbh, Docket No. C-4377, File No. 121 0081, Statement of the Commission, available at http://www.ftc.gov/os/caselist/1210081/121126boschcommissionstatement.pdf.

22 In the Matter of Motorola Mobility LLC and Google Inc., Commission Statement (Jan. 3, 2013), available at http://www.ftc.gov/os/caselist/1210120/130103googlemotorolastmtofcomm.pdf.

23 547 U.S. 338 (2006).

24 757 F.3d 1286 (Fed. Cir. 2014).

25 Id. at 1332.

26 Id.

27 Id.

SSOs to give licensees the option to license FRAND-encumbered patents essential to a standard on a cash-only basis and prohibit the mandatory cross-licensing of patents that are not essential to the standard or a related family of standards, while permitting voluntary cross-licensing of all patents. DOJ also has asked SSOs to establish procedures that seek to identify, in advance, proposed technology that involves patents which the patent holder has not agreed to license on FRAND terms and consciously determine whether that technology should be included in the standard.

While SSOs have not widely adopted all of DOJ's recommendations, they have started modifying their policies to account for the competitive effects of SEPs. The Institute of Electrical and Electronic Engineers (IEEE) recently announced proposed revisions to its patent policy regarding commitments from parties holding patent claims that are essential to IEEE standards to license those claims on FRAND terms. The update addressed the availability of injunctive relief, stating that participants "shall neither seek nor seek to enforce [an injunction]... unless the implementer fails to participate in, or to comply with the outcome of, an adjudication, including an affirming first-level appellate review... by one or more courts that have the authority to determine Reasonable Rates and other reasonable terms and conditions; adjudicate patent validity, enforceability, essentiality, and infringement; award monetary damages; and resolve any defenses and counterclaims."[28] IEEE also updated the meaning of a "reasonable" licensing rate, defined the permissible requests for reciprocal licensing, and established new production levels to which the commitment may apply. On 2 February 2015, DOJ announced that it would not challenge the proposed changes[29], and IEEE promptly voted to approve them.

SEPs and Antitrust in Europe

The potential for abuse of dominance in the context of SEPs has also been an area of increasing interest in Europe, with the competition authorities and courts across the EU attempting to strike the right balance between the fundamental rights to property and access to the courts of the SEP holder on the one hand, and the freedom of those seeking to implement the standard to conduct business on the other. For their part, in order to ensure that standardised technology is accessible to all interested parties under reasonable conditions, SSOs like ETSI[30] require that patent holders commit to license their SEPs on FRAND terms. Nevertheless, the conduct of SEP holders who have given such a commitment has given rise to a plethora of actions before the courts of several Member States. These have been based not only on competition law but also on civil law, and have given rise to a number of divergent legal approaches. This has resulted in a considerable degree of uncertainty as to the lawfulness of certain behaviour by SEP holders and companies which, in implementing the relevant standard, seek to use the teaching of an SEP.

Through its decisions in two investigations into the so-called "smartphone patent wars," the European Commission has sought to clarify the circumstances in which injunctions to enforce SEPs can be anti-competitive under EU law. The investigations in question centred on whether Motorola[31] and Samsung[32] had abused their dominant position by seeking injunctions to prevent the alleged infringement of their patents essential to the 2G and 3G mobile and wireless communications standards respectively. Accepting binding commitments from Samsung and reaching an infringement decision against Motorola, the Commission reached a similar conclusion to the US courts and FTC, namely that it is anti-competitive to use injunctions in relation to SEPs where, in a standardisation context, an SEP holder has committed to license the SEP on FRAND terms and the licensee is willing to take a licence on such terms.

In response to the obvious question of what then constitutes a "willing" licensee, the Commission was quick to point out that this will need to be assessed on a case by case basis taking into account the specific facts. However, the Motorola and Samsung decisions do already make clear that companies will be deemed "willing" licensees where, in case of dispute, they are willing to have FRAND terms determined by a court or arbitrators (if agreed between the parties) and to be bound by such a determination. Indeed under its commitments to the Commission, Samsung is bound not to seek injunctive relief in the EEA for 5 years against any company that agrees to a licensing framework

28 Letter from Renata Hesse to Michael Lindsay, Feb. 2, 2015, available at http://www.justice.gov/atr/public/busreview/311470.htm.

29 Id.

30 The European Telecommunications Standards Institute.

31 Case COMP/C-3/39.985 – Motorola – Enforcement of ETSI standard essential patents, Commission Decision of 29 April 2014.

32 Case AT.39939 – Samsung – Enforcement of UMTS Standard Essential Patents, Commission Decision of 29 April 2014.

providing for third party determination of FRAND terms by a court or arbitrators if no agreement can be reached on such terms through negotiation. Moreover, the Commission has stressed that such a licensee would not become "unwilling" if they were to challenge the validity, essentiality or infringement of SEPs.

The Commission's word is unlikely to be the final one on this matter. A ruling from the Court of Justice is expected later this year in the context of the SEP-based litigation between Huawei and ZTE linked to the next generation of wireless technology, the long term evolution (LTE) standard developed by ETSI[33]. Advocate General (AG) Wathelet's opinion of November 2014[34] had much in common with the Commission's position, holding that an SEP holder will abuse its dominant position if it seeks an injunction in circumstances where (i) it has given a commitment to the relevant standardisation body to grant third parties a licence on FRAND terms; and (ii) it can be shown that it has not honoured that commitment even though the infringer has shown itself to be *"objectively ready, willing and able"* to conclude such a licensing agreement.

AG Wathelet's opinion went on to provide more detail on the various steps that an SEP holder must take prior to bringing an action for an injunction if he is to avoid abusing his dominant position. These include making a written FRAND offer to the alleged infringer containing the precise amount of royalty requested and the way in which that amount is calculated. For its part, the infringer must respond to that offer in a diligent and serious manner if he is to be considered *"objectively ready, willing and able"*, including by promptly presenting a reasonable written counter-offer if he does not accept the SEP holder's proposal. The AG, like the Commission, considered that a licensee who – during the negotiations of a FRAND licence – reserves the right subsequently to challenge the validity, essentiality or infringement of SEPs, should not be considered "unwilling".

Conclusion

The intersection of competition law and IP law in the context of SEPs has become increasingly clear on both sides of the Atlantic over the past two years, and the rules of the road are becoming more clearly defined. For example, successful injunction actions on SEPs will likely be increasingly rare in the US. In Europe, on the other hand, while the AG's opinion provides more detailed guidance on the circumstances in which it may be anti-competitive for an SEP holder to seek an injunction enforcing its SEP, it remains to be seen whether the Court of Justice will follow the approach set out and what knock-on impact (if any) that will have on the patent policies or rules of SSOs in the EU. Either way, the Court's final ruling later this year should pave the way for a welcome harmonisation of this issue across the EU going forward.

This area will also continue to evolve as SSOs adopt new IPR policies to deter and prevent anticompetitive hold-up, and patent holders will assuredly continue to find creative ways to maximize the monetary value of their SEPs. Moreover, there are still several important issues that remain at least somewhat unresolved, such as the proper method of determining a "FRAND" royalty rate in a specific case. In short, the ICT sector will remain in the crosshairs of competition enforcers on both sides of the Atlantic for the foreseeable future.

Logan M Breed
Partner, Washington D.C.,
T +1 202 637 6407
logan.breed@hoganlovells.com

Angus Coulter
Partner, London
T +44 20 7296 2965
angus.coulter@hoganlovells.com

Sophie Bouckaert
Senior Associate, London
T +44 20 7296 2716
sophie.bouckaert@hoganlovells.com

33 Case C-170/13 - Huawei Technologies Co. Ltd v ZTE Corp., ZTE Deutschland GmbH.

34 Opinion of AG Wathelet in Case C-170/13, delivered on 20 November 2014.

Mexico's spectrum policy for 2015

The recent Federal Telecommunications and Broadcasting Law (the "Law") provides that the Federal Institute of Telecommunications (the "Institute") shall issue no later than the last day of each year, a program of frequency bands that will be auctioned and assigned in the following year.

In this sense, on December 30, 2014, the 2015 Annual program of use and development of frequency bands (the "Program 2015") was published in the Federal Official Gazette ("FOG"). It is the first time that the Institute applies this new figure and its main purpose is to grant certainty to the industry with respect to the frequencies that will be auctioned and assigned within the next year. This is an improvement vis-à-vis the old regulatory framework, since in the past there was no obligation to issue the program each year, as it was a discretionary decision of the regulator.

The Program 2015 details the bands, services, use and geographic coverage. The new Law classifies the spectrum concessions (including telecommunications and broadcasting) by their use as follows: (i) commercial use; (ii) public use; (iii) private use, and (iv) social use.

The main features of the Program 2015 are summarized below:

1. The Program 2015 envisages the following three auctions of frequency bands for commercial use for the provision of telecommunications services, which final award shall be issued within the course of this year:
   (i) Frequency bands 1710-1725/2110-2125 MHz (2 x 15 MHz), which are destined for the provision of mobile wireless access (broadband) with national geographic coverage within the 9 regions in which Mexico is divided. This block was not awarded in the last bidding process conducted in Mexico for telecommunications services (Bidding No. 21) in 2010. As this band is standardized for LTE, there is already a well-established ecosystem with considerable economies of scale.
   (ii) Frequency bands 1755-1770/2155-2170 MHz (2 x 15 MHz), which are also allocated for the provision of mobile wireless access with the same coverage and features of the prior band (LTE services and economies of scale). This block was reserved in the program of 2008. The Institute considers that this segment and the previous sum up 60 MHz, which could be considered very attractive for the entry of new players in the market.
   (iii) Frequency bands 440-450 MHz (2 x 5 MHz), attributed for the provision of capacity for private radio communications systems within 65 local areas in Mexico. This band shall be used exclusively to provide spectrum capacity on a wholesale basis to third parties seeking to implement a private radio system and the Institute shall implement mechanisms to clear the band and reallocate current users in the band. It is the first time in Mexico that a band will be auctioned for this purpose.
2. The Program 2015 also provides the auction of frequency channels within the band 88-106 MHz for commercial use for radio broadcasting services (FM) in 97 cities or towns within 18 States of Mexico (out of 32). The Institute will begin this bidding process during the second half of 2015.
3. In addition, the Program 2015 establishes the possibility for the Institute to directly assign some frequency bands for public use in (i) telecommunications for trunked and conventional radio services (415-420/425-430 MHz and 806-814/851-859 MHz) and (ii) broadcasting services (535kHz-1605kHz/88MHz-106MHz/470MHz-608MHz), subject to the coverage and other factors.
4. Finally, the Program 2015 sets forth some frequency bands that could be directly assigned by the Institute for social use in telecommunications and broadcasting services:
   (i) Frequency bands 824-849/869-894 MHz for the provision of mobile communications services in localities of up to 2500 inhabitants in 8 regions (except region 9) of Mexico in different blocks, which applications can be submitted at any time.
   (ii) Frequency channels within the band 88-106 MHz for radio broadcasting services (FM) in 18 cities or towns within 10 States of Mexico (out of 32), with limited coverage considering the type of station (as the case may be) and which applications shall be submitted within three specific periods depending on the location.
   (iii) Frequency bands 106-0108 MHz/1605-1705 kHz are reserved for communities or indigenous radio services.

According to the Law, any interested party may request on or before February 12, 2015 (30 business days), the inclusion of additional or different frequency bands and geographic coverage than those mentioned in the Program 2015. The Institute shall resolve the question within the following 30 business days, considering (among other) the following: the efficient use of the spectrum and infrastructure, the benefits to final users, the improvement of competition and the introduction of new and convergent services and applications.

The foregoing is in addition to the auction that the Institute is currently conducting for the creation of two new television channels with national coverage and the wholesale-shared network that the Government expects to develop in the 700 Mhz band through a public private partnership, which is in the process of being designed.

As time passes, the constitutional and legal telecommunications reform in Mexico is in the process of implementation by the Institute, such as the issuance of the Program 2015. It is a first step towards the allocation of new spectrum that the industry was demanding for long time. However, the real proof will be the completion of successful bidding processes, considering that the same will be conducted under new rules, authorities and market conditions not envisaged when the Program 2015 was prepared.

Indeed, the Mexican mobile market has experienced important changes, basically through the entrance of AT&T, who acquired Iusacell last year and Nextel this year. Instead of four, now there are only three players with the following market shares: Telcel with 68%, Telefónica with 19% and AT&T with 13%. However, the foregoing also modified the allocation of spectrum bands and currently AT&T holds 108 Mhz, Telcel 77.5 Mhz and Telefónica 70 Mhz. It is expected that AT&T will not be able to participate in the mentioned auctions, unless it returns part of its spectrum.

Although the Institute hopes that the auction for the 1.7 GHz and 2.1 GHz frequencies will permit the entry of a fourth operator to the Mexican market, the experience in Mexico and other countries has shown that the path is not easy for new entrants. The new telecommunications regime and measures imposed to Telcel as preponderant agent, as well as the entry of AT&T could encourage some international operators to step in to Mexico but that will leave the current operators with no additional spectrum in the primary market.

Federico Hernández Arroyo
Partner, Mexico City
T +52 55 5091 0164
federico.hernandez@hoganlovells.com

Full Foreign Ownership of E-commerce Businesses Permitted in the Shanghai FTZ: But is it a Breakthrough?

Background

Foreign investors are now permitted to establish wholly foreign-owned e-commerce companies in the Shanghai (Pilot) Free Trade Zone ("FTZ"). Formerly, foreign-ownership in such entities was capped at 55% in the FTZ and therefore restricted to Sino-foreign joint venture companies.

Outside the FTZ, the cap on foreign ownership is still 50% pursuant to the Circular of the *Ministry of Information Industry on the Readjustment of the Classification Catalogue of Telecommunication Services* issued on 1 April 2003 ("Telecoms Catalogue") and the *Foreign Invested Telecommunications Enterprise Administrative Provisions* issued by the State Council effective 1 January 2002. In 2013, the Ministry of Industry and Information Technology ("MIIT") issued a draft new version of the Telecoms Catalogue, but it is unclear when or whether that will ultimately become law.

This change, which takes effect immediately, on a pilot basis, was announced by MIIT on 13 January 2015, in its Announcement on Lifting Restrictions for Foreign Equity in Online Data Processing and Transaction Processing Services (Operational E-commerce Businesses) in the Shanghai Free Trade Zone (关于在中国(上海)自由贸易试验区放开在线数据处理与交易处理业务(经营类电子商务)外资股权比例限制的通告) ("Announcement").

The Announcement means that foreign investors will be able to apply for *Value-added Telecommunications Services Permits* ("VATS Permits") that allow their wholly-owned subsidiary enterprises in the FTZ to engage in "e-commerce business". However, the challenge for foreign investors will be to work out what "e-commerce business" really entails.

E-commerce business

The precise meaning of "e-commerce business" is not defined in the Announcement or indeed in any other regulation. Under the Telecoms Catalogue, there is no standalone "e-commerce business" category. In the Announcement, MIIT seems to have categorized "e- commerce business" as part of the Online Data Processing and Transaction Processing Services ("OTP Services"), a Category One Value-added Telecommunications Service ("VATS"). OTP Services are defined broadly under the Telecoms Catalogue as "using all types of application platforms for data and transaction/business processing which are linked to a communications network to provide the customer with online data processing and transaction business processing through a communications network". Transaction processing services include banking services, share trading services, ticketing sales services, commodity auctioning services and payment services. "E-commerce" broadly means trading in products or services using computer networks, which fall within the broad definition of OTP Services set out above.

Logically, this should cover the sale of third party products through an entity's online platform. If that were the case, the pilot scheme heralded by the Announcement would then provide foreign investors with greater access to what many commentators believe to be the world's largest e-commerce market and create a more level playing field in which foreign-invested e-commerce companies can compete directly against the likes of Alibaba and JD.

However, based on our inquiries with MIIT, this is not necessarily the case. According to the MIIT official whom we spoke to, a separate VATS Permit under the Information Services Business category (commonly known as an Internet Content Provider Permit, "ICP Permit") a Category Two VATS is required for a website that is 'for profit' (经营性) (refer to the *Internet Information Services Administrative Procedures* issued by the State Council effective 25 September 2000 for a definition).

The MIIT official we spoke to said that advertising and search ranking services that generate fees would be considered 'for profit' activities for which an ICP Permit is required. He compared this to purely providing a platform for users (B2B, B2C and/or C2C) to list and trade their products or services for a fee, which does not require an ICP Permit. Importantly, foreign ownership in an entity holding an ICP Permit is capped at 50% (except for app stores in the FTZ where there is no cap – see below). The benefits for foreign investors are, therefore, limited, as most e-commerce operators derive a large part of their income from third party advertising. It also represents a possible shift in MIIT thinking: where our earlier enquiries with MIIT indicated that e-commerce involving the sale of third party products through an online platform was an activity requiring an ICP Permit rather than an OTP Services VATS Permit. In practice, we strongly recommend

consulting with the relevant MIIT authorities on the technical aspects of the operations to determine which categories one would fall under as interpretations can vary between different locations.

MIIT also made it clear that an e-commerce or OTP Services VATS Permit is distinct from an online payment processing permit from the People's Bank of China ("PBOC") (a "Payment Permit"). The rules governing Payment Permits issued by PBOC in 2010 make reference to separate rules governing foreign investment in the sector, but the latter have never been issued. PBOC officials have, however, recently told us that they welcome applications for Payment Permits from foreign investors. However, our understanding is that only two wholly foreign enterprises ("WFOEs") in China have obtained a Payment Permit (Sodexho and Edenred) – both for prepaid cards rather than Internet payment services.

Therefore, the new pilot scheme may mean that WFOEs in the FTZ that are able to obtain the requisite Payment Permit from PBOC may now also be able to obtain a VATS Permit allowing them to provide a full suite of online payments services through their own online platforms (payment services being part of the OTP Services from the MIIT perspective at least)[1] – thus allowing them to enter a business that has thus far largely been off-limits to foreign investors. That would, in turn, allow them to benefit from recent financial reforms allowing the provision of online cross-border RMB payment services in Shanghai.

Shanghai FTZ's continuing liberalisation in telecommunications

The Announcement follows MIIT's announcement a year earlier in January 2014, that it would allow greater foreign capital investment in seven types of valueadded telecommunications services businesses in the FTZ: Call Centre Services; Domestic Multi-party Communications Services; Internet Access Services; Domestic Internet Virtual Private Network Services; App Stores under Information Services; Store and Forward Services; and Online Data Processing and Transaction Processing Services. That removed the (50%) cap on foreign investment in all but two of these

1 It is subject to debate that whether third party payment organisations need to hold a VATS Permit. To see our commentary in this regard, please refer to "Third Party Payment Licences in China – Are They within The Grasp of Foreign Investors?"

businesses: Domestic Internet Virtual Private Network Services and Online Data Processing and Transaction Processing Services. For Domestic Internet Virtual Private Network Services, the cap remained at 50% – that remains unchanged. For Online Data Processing and Transaction Processing Services, it increased the cap only slightly, from 50% to 55%. It is that 55% cap that has been removed by the Announcement - clearly, the impact of the Announcement is not as significant as the measures taken in January 2014. In April 2014, MIIT issued further rules setting out the requirements and procedures for companies applying for VATS Permits in the FTZ.[2]

Foreign invested commercial enterprises

Apart from MIIT's grip on the e-commerce industry, as further background, the Ministry of Commerce ("MOFCOM") which is the primary regulator of foreign direct investment into China, has also sought to regulate e-commerce pursuant to the MOFCOM General Office Circular on Issues Related to Examination, Approval, and Administration of Online Sales and Vending Machine Sales Projects of Foreign-Invested Enterprises (商务部办公厅关于外商投资互联网、自动售货机方式销售项目审批管理有关问题的通知) effective 19 August 2010 ("Circular"). Under the Circular, MOFCOM does concede that a VATS Permit is required if the online platform is open to third parties (i.e. e-commerce). Importantly, the Notice does not clarify whether the type of VATS Permit required is one for OCP or ICP VATS. As a separate point, note that if the products sold on the platform are solely products of the online platform operator, only record filing with MIIT is required, as opposed to an actual VATS Permit. Interestingly, MOFCOM requires that foreign invested e-commerce entities will need to be established in the form of a foreign-invested commercial enterprise (外商投资商业企业) ("FICE"), which is a unique creature subject to MOFCOM approval introduced in 2004 under the Foreign Investment in the Commercial Sector Administrative Measures (外商投资商业领域管理办法). compared to when they were first introduced more than a decade ago. Nonetheless, this adds another layer of complexity for foreign investment into the e-commerce industry.

So does it really matter?

Historically, China has been extremely protective of its telecommunications sector and it has been relatively difficult for foreign-invested enterprises to obtain VATS Permits – even for those Sino-foreign joint venture companies who were entitled to apply for them. The Announcement, along with MIIT's earlier FTZ-specific rules, appears to indicate a move towards the relaxation of that protection. However, a more detailed analysis suggests less of a positive impact, because an ICP Permit is required for many business models, where foreign ownership is still capped at 50%.

As the generally positive news of the Announcement filtered into the market, any sense that things in this industry were moving in the right direction was tempered by the less positive news that several VPN operator services (which allow users in China to circumvent the 'Great Firewall of China' to access blocked overseas sites) were being blocked. The official (MIIT) explanation for this is that it is intended to promote the "healthy development" of the Internet. VPN is classified as a "basic telecoms service" under the Telecoms Catalogue. It is an area where foreign investment is permitted, subject to a 49% foreign ownership cap, but where no joint ventures have been approved (at least in the public domain) since China's accession to the World Trade Organisation.

The Internet and telecoms sectors remain very challenging for foreign investment. Given China already has well-funded e-commerce giants (Taobao, JD, Vancl and Yihaodian to name but a few) that are already in China and are seeking to expand overseas, the rationale for continued protection of the local industry from foreign competitors seems ever weaker and more difficult to justify. Nonetheless, the Announcement represents a welcome step in the right direction.

2 China (Shanghai) Free Trade Experimental Zone Foreign-Invested Operational Value-Added Telecommunications Services Administrative Procedures for Trial Operation (中国(上海)自由贸易试验区外商投资经营增值电信业务试点管理办法)issued by MIIT on 14 April 2014 and effective from the same date. For further information on this regulation, please refer to our client note "New Rules Provide a Framework for Shanghai FTZ to Open the Doors on VATS: A Cause for Optimism?".

Andrew McGinty
Partner, Shanghai
T +86 21 6122 3866
andrew.mcginty@hoganlovells.com

Anna Elshafei
Counsel, Shanghai
T +86 21 6122 3803
anna.elshafei@hoganlovells.com

Roy Zou
Partner, Beijing
T +86 10 6582 9596
roy.zou@hoganlovells.com

Kurt Tiam
Counsel, Beijing
T +86 10 6582 9555
kurt.tiam@hoganlovells.com

Mark Parsons
Partner, Hong Kong
T +852 2840 5033
mark.parsons@hoganlovells.com

Commercial Use of Unmanned Aircraft Systems (UAS)
A Brief "How-to" Guide

Overview
The commercial use of Unmanned Aircraft Systems (UAS) technology is at the cutting edge of the intersection of technology, law, and business. Companies around the globe are taking a hard look at their business plans to determine if it is appropriate to invest in UAS technology to tackle practical business problems. In many cases, companies are determining that use of UAS technology provides a solution. Areas with practical commercial application include energy, film making, infrastructure, agriculture, media, sports, education, emergency relief, real estate, hotels, and resorts, to name just a few. Unlike some more traditional and established technologies, the use of UAS for commercial purposes is based on a developing and uncertain legal foundation, one that must be viewed from a multitude of perspectives: aviation law, communications law, data privacy law, export law, and government security concerns, among others.

Industry-specific applications and related transactions

- Real estate
- Remote sensing
- Agriculture (crop/moisture monitoring)
- Sports
- Film making
- Energy (e.g. flare stacks)
- Border patrols/ drug enforcement
- National security
- Emergency and rescue

With this uncertain and developing legal foundation, companies planning to use UAS technology should ensure that they have obtained the necessary Federal Aviation Administration (FAA) and other regulatory authorizations, and consider contractual and legal risk mitigation techniques, whether the transaction is the creation of a joint venture, a merger or acquisition, or a commercial transaction involving the sale, purchase, or implementation of UAS technology. Any one of these UAS-related projects may require a collaborative effort with a close eye on budget and schedule risk mitigation considerations, while harnessing a proactive strategy to navigate the regulatory landscape. The opportunities are significant, but so are the regulatory challenges.

> "I don't pretend we have all the answers. But the questions are certainly worth thinking about."
>
> *Arthur C. Clarke*

Particular attention must be paid to contractual provisions that envision the allocation of risk and outcomes to accommodate the timing, incremental costs, requirements and limitations that are imposed as the law evolves. These provisions include risk and cost allocation (and adjustment) provisions, termination provisions, insurance availability, implications for existing financial covenants and financing availability, flexibility of technology infrastructure to accommodate new legal requirements, as well as sufficient provision in business planning (and related agreement provisions) to allow for increased costs necessitated by new legal requirements.

Considerations for UAS transactions
Regulations concerning UAS are emerging, with new developments every month. While the principal regulator of UAS in the United States is the Federal Aviation Administration (FAA), the Federal Communications Commission (FCC) regulations are also important, as is privacy regulation. State regulation of UAS is emerging in parallel, as exemplified in the ongoing legal developments in the State of California, where many emerging UAS businesses are located. For many companies, commercialization of UAS also needs to be considered with an eye toward export regulation and international legal requirements. Global regulation of UAS is evolving in parallel, and sovereign legal regimes are diverse in their state of development, which makes a "one-size-fits-all" solution that much more challenging for a global system architecture.

In this emerging industry, it is vital that before entering into any UAS transaction, stakeholders are fully updated on the current state of the applicable

law and anticipated changes in the law. It is equally important that the contract provides for protection in the event of changes in law, especially in the provisions related to compliance with applicable law, cost of compliance and the resulting actions that are to be taken if the literal provisions of the contract cannot be carried out due to changes in law.

Due diligence
A full understanding of the legal framework (existing and anticipated, federal, state, and international) is necessary as applied to the intended operation(s) of the UAS. This will be necessary to evaluate project feasibility, assess the costs and limitations, and for consideration of the contractual provisions that will be required to adjust to changes in the legal framework.

Unlike most settled areas of law, in the case of UAS, gauging risks and negotiating contractual provisions to allocate that risk in view of the changing legal environment presents a significant challenge. Understanding the existing legal landscape, which may in turn be based on the intended system architecture, is a key first step to a successful transaction. The business plan, operational assumptions, technological flexibility, and adaptability (and the cost thereof) must be considered against both the existing and potential changes in the legal landscape.

Contractual provisions
A series of special contractual provisions should be considered in drafting a commercial agreement for a UAS transaction, including the following:

Regulatory conditions precedent or subsequent to having a transaction
Consideration should be given as to whether obtaining a regulatory authorization is a feasible path at all, and whether the timing of the transaction (and/or off-ramps) can be based on obtaining a regulatory authorization, or instead waiting for changes in applicable law to permit implementation. This may depend on the state of the law, and the exemptions granted at the time the transaction is entered into, as well as the technology, relevant jurisdictions, and legal issues raised by the specific proposed UAS operation. The parties should consider if the risk of whether the transaction can occur at all may be addressed in an acceptable manner through conditions precedent or subsequent, including transactional termination and/or indemnification provisions relating to receipt of a regulatory authorization or obtaining needed regulatory changes, or rights of either or both parties to make adverse determinations (off-ramps) with regard to implementation of the business plan in the absence of regulatory action over a defined period.

Schedule for determining if there is a deal
Many UAS-related projects will be time and sweat equity dependent. Parties entering into a commercial transaction should be willing to invest a substantial amount of time, recognizing that a solution provided by UAS technology requires a commitment. Parties should consider having firm backstops to the development or implementation timeline, and consider the remedies if that timeline is not met.

Funding the start-up phase
Investors may initially be wary of an untested commercial technology, particularly with uncertain and shifting regulatory hurdles. Therefore, investors may seek to add additional layers of contingencies to funding UAS-related

Silicon Valley

A number of technology companies have been exploring and testing the use of UAS for several years. For instance, Google X began working on UAS technology in 2011, and conducted a test flight on a farm in Australia in 2014. Google also acquired Titan Aerospace in 2014. Titan makes high-altitude, solar-powered UAS that can stay aloft for 5 years without the need to land or refuel. These UAS have many different potential uses, and Google has recently requested permission from the FCC to conduct UAS tests to identify the potential for using these UAS to deliver internet to remote areas. In light of the unsettled U.S. regulatory regime governing commercial UAS use, technology companies have been aggressively advocating and lobbying for clearer rules that would permit commercial applications of the type contemplated by these technology companies. Amazon has been in the forefront of advocacy for such rules among technology companies. In March 2015, the company received initial and limited approval from the FAA to test UAS near its headquarters in Seattle, Washington. Amazon has been testing UAS deliveries in the United Kingdom and says that it will expand research in the United Kingdom and outside of the country if the U.S. government does not loosen its grip on flight testing restrictions. Other technology companies are contemplating using UAS in consumer applications that may also draw regulatory scrutiny.

programs, such as terms and conditions with timeframes for development, delivery, and implementation. Investors' requests need to be carefully considered and addressed early in the process, to limit surprises or delays as the program or deal progresses.

Advocacy with regulatory bodies and dealing with unexpected decisions

For companies desiring to operate UAS for commercial purposes, active participation in the process of seeking FAA authorizations, regulatory interpretations or approvals may be required. Contract parties, whether in M&A transactions, investments, joint ventures, or other transactions, are accustomed to contracting around risks that regulatory approvals will not be granted and allocating responsibilities for seeking approval. Since the FAA UAS rulemaking process is anticipated to be a lengthy one, specific provisions will be needed to address the roles of the parties in seeking the necessary FAA authorizations and the parties' rights to shape the applications for such authorizations. This is particularly important where a denial of such an application may be preferred by one or more parties over the grant of an exemption that comes with high compliance costs, and thus obligates the parties to move forward, but perhaps with different economics than originally anticipated. There are some analogous provisions in the commercial lawyer's bag of tools, such as provisions dealing with divestitures for merger approvals or for payment of break-up fees if conditions attached to approvals are beyond described limits. Fashioning such contractual provisions to handle unknown regulatory risks is therefore critical for UAS transactions, especially since the possible outcomes are not predictable, and there is no body of precedent to look to for risk assessment guidance.

Allocating responsibilities for and costs of compliance with laws not yet known

The regulatory landscape may well evolve over time to support broader commercial operations of UAS than will be available through the FAA's exemption process. Where the parties are prepared to put a temporary arrangement in place while awaiting broader regulatory

action, there may well be costs of compliance that exceed those that will apply when the regulations are fully developed. For example, the FAA may impose more stringent requirements as a condition of granting an exemption than would apply under generally applicable rules, including technology requirements (such as technology to ensure the UAS's avoidance of other UAS or manned aircraft), pilot certification and training requirements, operational restrictions such as visual line-of-sight requirements, and privacy-focused requirements (such as limitations on operations over another's property without the owner's consent).

In the event of an ongoing partnership with another entity, whether through commercial contract or joint venture, the transaction documents ideally would contain an obligation for each party to comply with applicable law, even as the law may change over time and between jurisdictions worldwide. However, with UAS this is not as simple as compliance with other more established legal requirements, such as anti-bribery statutes, Foreign Corrupt Practices Act, (FCPA) or export requirements (e.g., ITAR). Regulatory checklists and timeframes should be kept in mind. Ideally, specific compliance obligations would be addressed directly as specific obligations of the parties, so that failures can be conditions to performance by other parties, and costs of compliance can be factored into the economics of the arrangements.

In a sale transaction, does the buyer or seller agree to fund the costs of product modifications to achieve legal compliance, as of what date or on an ongoing basis, and based on what standard? What might the compliance upgrade entail? Is the UAS inexpensively and easily upgradable, for example, remotely through a software change, or would there be a need for a return to the seller for a software and/or hardware upgrade? Who will be liable for continued operations without the upgrade, including with respect to continued sales under an existing contract? Can the contract terms continue to be fulfilled (while appropriately allocating liability and imposing any necessary indemnification) and/or provide for termination at the discretion of either party in the case of a failure of the basic assumptions about operational feasibility? Does (and should) the contract limit the geographic area of sale and usage of a UAS to a location where the same is lawful, and what liability exposure is there to each party to the transaction if the UAS is operated in an unlawful manner in the applicable jurisdiction? When is a contractual termination right the appropriate remedy, with or without additional economic payments,

indemnification or forfeitures, and to be exercised by which party (or both parties) to the transaction?

These costs of compliance cannot readily be estimated in the absence of specific regulatory standards and requirements or even reliable predictions as to what those standards and requirements will be, yet in order for a meaningful, binding arrangement to exist, those costs and burdens of compliance will need to be allocated. The issues involved in allocating these risks, and the costs resulting from changes of law in this area, present the greatest challenges in developing a contract structure that addresses the interests and reasonable expectations of all parties to the transaction. At a minimum, a combination of cost and risk allocation provisions (possibly with provisions for equitable adjustment) and termination provisions if there are major departures from the parties' assumptions about compliance costs may prove advisable.

Software upgrades and expenses

Particularly with regard to the purchase of UAS technology, the buyer will seek to have the seller take responsibility for the cost of software upgrades and expenses, and the reverse will be true for the seller, particularly in a firm fixed-price environment where unknown upgrades may be required. Regardless of how the commercial deal is ultimately struck, there needs to be a path for the buyer to oblige the seller to perform the upgrades either as part of the underlying agreement (if the law changes prior to delivery), under an ongoing warranty provision, as a firm fixed-price option, or otherwise on an equitable adjustment basis. Since the potential compliance modification costs may be difficult to foresee, the seller will need to consider pricing such updates appropriately, whether into the base contract, through options, or through an equitable adjustment provision.

In the event that a hardware change is required, or the software is not amenable to a self-installed upgrade, the costs of compliance become much more significant, as does the proper consideration and allocation of such costs in the contract.

In the context of a joint venture or acquisition transaction, the amenability and flexibility of the UAS platform to least-cost upgrades to accommodate changes in law, diversity of spectrum allocation for telecommunications, and other evolutionary improvements all need to be considered in the business model and transaction pricing for the project.

Allocating liability for legal but "unsafe" activity

The more UAS that are deployed, the more important it will be for those UAS to coexist safely with other UAS and with general aviation and commercial aviation aircraft. This will likely require the development of both new air traffic control capabilities and safety regulatory standards and operational requirements for the various types of UAS (perhaps with differing standards and requirements applying to different types of UAS, depending on their complexity, characteristics, and capabilities, as well as the purpose, location, and altitude of the UAS operation).

Entering into arrangements in advance of adoption of the standardized safety standards may require dealing with the real possibility that a proposed UAS operation business model will not be contrary to any enacted UAS safety regulatory standards or operational requirements, but still could be deemed "unsafe," giving rise to significant liability risks in the case of interference with manned aircraft or other UAS, or injury or damage to individuals or property. The legal standards by which these activities will be assessed as to negligence, strict liability, and other legal theories are not yet developed, and may in fact be viewed differently across different jurisdictions. Those risks may currently be uninsurable, leaving the parties to handle the risks among themselves.

Indemnification

Once there is agreement on the allocation of liabilities and risks, the parties need to support that agreement with appropriate indemnification provisions by the responsible party. Counsel will need to advise on whether to draft these provisions narrowly, simply to handle identified risks, or whether to have broader indemnification should the government or third parties seek redress based on theories not yet determined. Even if a sales agreement for a UAS allocates liability to the seller, or a joint venture agreement limits liability to the joint entity, in all likelihood the government and/or third parties may proceed against all parties to the contract or joint venture. It is therefore critical to consider these provisions, often considered "boilerplate" in more routine arrangements, with great care. It is also vital to try to predict the compliance risks, first by understanding the potential consequences and risks of potential violations of such regulatory regimes, and then building into the transaction the remedies and potential termination that results in the event of a compliance enforcement issue.

UAS in action: Sports

UAS presents an opportunity for ski resorts to obtain high-quality aerial images and video of skiers and ski races. Their most prominent use as of yet has been to promote ski locations through social media. Last summer, New Zealand Tourism launched the #nzdronie promotional campaign. Its UAS shot 8-second HD clips of visitors at several New Zealand South Island ski areas, then emailed the free videos ("dronies") to participants to allow sharing on social networks. This campaign was very popular. In the United States, some companies and individuals are beginning to use UAS to document ski races. In the future, ski resorts may use UAS for mountain search and rescue operations.

In the United States, ski resorts may be able to obtain FAA exemptions for UAS commercial use in order to use UAS to document races or assist with safety issues. The FAA has already issued a number of such commercial use exemptions, including for photogrammetry and crop scouting for precision agriculture and to augment real estate listing videos.

If the transaction counterparty is a start-up or less well-funded entity, care must be taken to best structure the deal with other contractual protections in the event that the indemnity provisions prove to be of little or no practical benefit. For example, consideration should be given as to including provisions requiring ongoing disclosure and visibility as to operations to ensure compliance, insurance (if obtainable), performance bonds, escrows or modified payment schedules, and the right to terminate the contract for default in case of violation of law by the counterparty.

Mechanisms to effect modifications to accommodate changes in law

Most contracts or other similar legal relationships are based upon a concept that there be a "meeting of the minds," without which a court will not enforce the arrangement. Other doctrines such as commercial impossibility also could potentially come into play. The parties should assess whether the commercial contract approach should be used at all where the legal rules eventually adopted could be quite different than what the parties presently believe will be the case. For a contract to survive a "no meeting of the minds" challenge, or to keep risks at manageable levels, the parties may well need to implement adjustment mechanisms to maintain the basic economic deal between the parties. There are some standard mechanisms for contract adjustments to deal with the economic changes over time (such as escalation provisions, based on pricing indices) or changes to the obligations of the parties to provide services or usable products (such as a directed changes clause, where changes can be directed within the general scope of the contract with an "equitable adjustment" to the price, schedule, or other terms). Would either of these adjustments work where the basic permitted ground rules for a project are not currently known? For any chance to have a binding arrangement without undue risk, a series of risk allocation and adjustment provisions, coupled with termination rights, buy-sells, or other off-ramps to cap maximum exposure, may be the best way to manage this level of uncertainty.

A joint venture or partnership arrangement, where the parties agree to conduct business together even if things do not evolve as anticipated, may be a sturdier vehicle for handling the high level of uncertainty. If there is a significant change of operation, business purpose or cost based on modifications to the law, rather than having economic adjustment provisions to accommodate the legal changes the parties could employ various rules of governance to alter the business model. Of course, as with any governance provisions there are issues about the required level of support, including level of approval (majority, supermajority, or unanimous) and capital contributions to be made by the parties. Again, a combination of decision mechanisms with off-ramps (dissolution provisions, buy-sells, or limits on overall liability) to protect the parties against situations too far from the envisioned business model may be the best alternative.

Whether the transaction is a "simple" commercial contract or a more complex joint venture or corporate acquisition, significant thought needs to be given as to termination or modification of the transaction based on changes in the law. Thinking these issues through is critical, and it may be to your advantage to seek agreement at the onset to set the parties' expectations as to the costs and liabilities, rather than leaving the implications of changes to later negotiations. All reasonable scenarios should be contemplated in drafting agreements, to ensure that the compliance,

approvals, costs, indemnification, termination, insurance, and financing provisions (among others), support the desired business outcome.

Product liability and insurance

Regardless of the type of transaction, the liabilities and insurance provisions, with respect to third parties as well as property risk of the technology itself, should be carefully taken into consideration.

This includes identifying responsibility for providing appropriate instruction manuals, labeling of UAS as to risks, and other standard commercial liability practices for risk allocation.

Commercial industry participants utilizing UAS technology will need to work closely with underwriters to obtain the required protection to mitigate loss, both through requirements of insurance carried by counterparties and your own company. As the industry evolves, and given anticipated exclusions, there may be some losses that are not immediately insurable. Particularly in commercial transactions, these liabilities need to be clearly articulated between the parties.

Litigation

Clear termination and force majeure provisions in the event of changes in law that make performance untenable for one of the parties can help stave off litigation. So too can carefully crafted indemnification and change- and upgrade- cost allocation provisions. Parties should also give careful consideration to warranty rights and obligations and related disclaimers, as well as limitation of damage provisions. Bear in mind that contractual limitations of liability and damages provisions are useful tools for dealing with disputes between contracting parties, but less helpful in the event of third-party claims, for which an indemnification regime is a better tool to allocate risk. In short, the more the parties can do to anticipate and plan for areas of potential dispute up front, the less likely they are to end up in litigation.

But even under carefully constructed contracts, disputes will arise. As a result, choice of law and forum should be focused upon in connection with any commercial UAS project, because outcomes of similar disputes may be different under different legal regimes, both within the United States and around the world.

Careful consideration should also be given to the use of alternative dispute resolution procedures, such as

arbitration. Where the parties' legal rights turn on a determination of the current state of regulation (as opposed to just contractual intent), it may be challenging to find an arbitral panel with the legal expertise to make such determinations. An arbitral decision in such cases may not be fully in line with a federal agency viewpoint, and in such cases a judicial decision may provide a better and more definitive result. In determining whether to incorporate alternative dispute resolution procedures into a transaction, the relevance of regulatory expertise in potential disputes should be weighed carefully, as well as the pros and cons of the publicity and precedential effects of proceeding in a judicial forum, and the potential availability of injunctive relief not available in arbitration. For cross-border transactions, the challenges are even more complex, with an added layer of issues around the enforceability of judicial decisions and arbitral awards in foreign forums.

In all cases, it will be critical to ensure that the parties understand how the choice of law and forum selected in a heavily regulated and evolving environment may drive the resolution of disputes. The parties also must contemplate how that legal backdrop, their resulting rights and obligations, and the outcome of their disputes, can all shift with changes in the law. Care needs to be taken as to the critical provisions that may be affected by the changes in law to ensure that the correct outcome in fact is to be derived from the agreement provisions as drafted.

FAA authorization, regulation, and enforcement

The FAA published in the Federal Register its Notice of Proposed Rulemaking (NPRM) on Small UAS (less than 55 pounds) on 23 February 2015, but the FAA's firm position is that until the Final Rule on Small UAS is issued (which is likely two or three years away), no business may operate a UAS for commercial purposes, including using a UAS as a business tool (regardless of whether compensation is received), without obtaining specific prior authorization from the FAA. Such authorization may come from either (a) obtaining an FAA certificate of airworthiness for the UAS and complying with all applicable Federal Aviation Regulations (FAR), or (b) obtaining an FAA regulatory exemption under Section 333 of the FAA Modernization and Reform Act and a "private" Certificate of Waiver or Authorization (COA). For most UAS, obtaining a certificate of airworthiness is neither practical nor cost-effective. In order to obtain a Section 333 regulatory exemption and a private COA, the applicant must file with the FAA a petition for exemption and an application for a private COA.

While the FAA permits an applicant to file such a petition and application without discussing the matter with the FAA first, the wiser course is to meet with the FAA and discuss the proposed UAS operation before finalizing and filing these documents. The timing of the filing is an important business consideration. The FAA processing time for the Section 333 exemptions it has granted typically has been in the range of four to eight months. With a large backlog of Section 333 petitions for exemption developing at the FAA, that processing time is likely to grow in the future. For that reason, companies contemplating using UAS for commercial purposes should plan for long processing times, and file as soon as reasonably possible.

Many companies appear to be under the mistaken impression that the FAA does not regulate or require authorization for commercial uses of Small UAS that operate at low altitudes and without any compensation being earned for the operation. The FAA is addressing this lack of understanding primarily through an aggressive education program. Nevertheless, the FAA has indicated through recent pronouncements that it

Energy

Energy companies across the world are already utilizing and testing UAS. Oil and gas companies are using and testing UAS to survey land, monitor pipelines, and monitor drilling rigs, particularly in areas where harsh weather makes conventional monitoring difficult.

In June 2014, the FAA approved a plan by energy corporation BP and UAS manufacturer AeroVironment to use UAS to conduct aerial surveys and monitor pipelines in Alaska's Prudhoe Bay oil field. Royal Dutch Shell is conducting similar surveys over Arctic waters. U.S. wind energy companies are exploring the use of UAS to inspect wind turbines and blades.

In Canada, a number of oil sands companies, including Royal Dutch Shell and Syncrude Canada Ltd., are using UAS for surveys and mapping. And oil and gas companies are using UAS internationally to monitor pipelines for leaks and vandalism.

FAA exemptions for commercial use of unmanned aircraft systems

The FAA has received hundreds of Section 333 petitions for exemption for commercial UAS operations, with more being filed practically every day. The FAA has granted dozens of exemptions, and is issuing more virtually every week. The exemptions have covered UAS operations for many different purposes, including:

1. movie and television production;
2. precision aerial surveys;
3. aerial imaging of construction sites;
4. flare stack inspections of overwater oil production platforms;
5. conducting photogrammetry and crop scouting for precision agriculture;
6. augmenting real estate listing videos and enhancing academic community awareness of the local area for those unfamiliar with the area; and
7. aerial photography and inspections.

Conditions to these exemptions have typically included requirements that:

- the UAS operator hold a private pilot certificate;
- the UAS be kept within line of sight of the operator at all times;
- the UAS be inspected before each flight;
- there be no night UAS operations; and
- the UAS be operated at 400 feet above the ground or lower.

In issuing these exemptions, the FAA has emphasized the importance of the manuals covering UAS operations, maintenance, and inspection procedures that have been submitted by the petitioners. For exemption holders, the FAA issues "private" Certificates of Waiver or Authorization (COAs) that set forth UAS flight rules and require timely reports of any accidents or incidents involving the covered commercial UAS operations.

is prepared to take enforcement action against anyone "who conducts an unauthorized UAS operation or operates a UAS in a way that endangers the safety of the national airspace system." The FAA can and does issue warning letters and letters of correction, and may seek civil penalties for such operations, particularly where the FAA believes that the operator knew its conduct constituted a violation. The FAA has indicated that the higher the risk to safety posed by the unauthorized UAS operation, the higher will be the penalty imposed by the FAA. For those individual operators who hold an FAA certificate, this penalty may include the FAA's suspension or revocation of the certificate. The FAA also has issued guidance to local law enforcement agencies to encourage them to assist the FAA's UAS enforcement activity, and to inform these agencies of steps that they can take to identify violators and gather evidence for use by the FAA.

For companies considering using UAS for commercial purposes, taking into account these FAA authorization, regulation, and enforcement issues, and ensuring full compliance, will be essential to a successful business transaction and rewarding commercial UAS operation.

FCC considerations

Virtually every UAS will avail itself of wireless communications for command and control purposes (i.e., directing or controlling the flight of UAS). Additionally, UAS will likely require communications to allow concurrent operations with other, ubiquitously deployed UAS-potentially under, as it evolves, a central safety control system. These wireless communications subject the UAS to FCC jurisdiction, and companies must consider issues including: (a) identifying appropriate licensed or unlicensed spectrum for the UAS; (b) acquiring spectrum licenses, if necessary; (c) applying to certify UAS as wireless transmitters under the FCC's "equipment authorization" process; (d) evaluating whether any fixed wireless infrastructure is required, which itself requires FCC approval; and (e) ensuring ongoing compliance with the relevant FCC technical rules, including avoiding interference to protected wireless operations.

As companies evaluate transactions involving UAS technology, each of these considerations will present significant risks and considerations. The FCC has stepped up enforcement for violation of its rules, and failure to comply presents steep penalties. The framework for the UAS should include a clear plan regarding what type of spectrum (licensed or unlicensed) it will use and, if relying on unlicensed spectrum, ensure that it meets quality of service (QoS) requirements. All

UAS wireless equipment should be certified under the FCC's equipment authorization process, and companies should be able to demonstrate compliance with FCC technical rules. If a company holds FCC licenses prior to a change in control of the entity, the parties must make sure they seek approval with the FCC regarding the transfer of the license. Considering these and related issues at the beginning of any UAS-related transaction will help ensure its success and avoid significant repercussions or disappointment at a later time.

Export and trade regulation matters

In addition to general provisions as to compliance with law, the agreements will need to contemplate: (i) obtaining any requisite trade (including export) licenses or exemptions as a precondition to certain transactions (as required for compliance or to monitor ongoing compliance); (ii) obligations to cooperate on obtaining and maintaining approvals; and (iii) time frames for approvals to be received.

These provisions will be most applicable in cross-border sales, joint ventures, and corporate acquisitions involving parties in multiple jurisdictions and should be expected to present more significant hurdles depending on the jurisdictions of the parties, the sophistication of the technology, and the government versus commercial nature of the project.

Thirty-four countries, including the U.S., are members of the Missile Technology Control Regime (MTCR), "an informal and voluntary association of countries which share the goals of non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction," that restricts the sale of armed and unarmed UAS due to missile technology proliferation concerns. Consistent with its MTCR commitments, the U.S. and other member country governments have in place restrictions on exports of UAS vehicles, components and related technology. The U.S. government in particular has a comprehensive export control program for UAS. The State Department has export licensing jurisdiction under the International Traffic in Arms Regulations (ITAR) for defense articles and services covered by the U.S. Munitions List (USML), including all military and armed UAS, regardless of range or payload, and certain UAS software, components, and technologies. The Department of Commerce has export licensing jurisdiction under the Export Administration Regulations (EAR) for dual-use items on the Commerce Control List (items with civilian and military applications) – these can include certain UAS and related equipment, software, and technologies that are of missile technology proliferation, national security, and other concerns but not already controlled on the USML. Companies should carefully consider the coverage of U.S. and other export control regimes when contemplating any proposed transaction that will involve UAS exports.

Intellectual property

As in all areas of evolving technology, for UAS-related technology too, great care needs to be taken to understand, define, and allocate the ownership of intellectual property (IP) rights in the technology, to protect the IP rights in the technology, to diligence, and to consider third party IP rights in the technology prior to undertaking both commercialization, and the later permitted uses and licensing of the technology.

Consideration of the ownership of IP rights in UAS-related technology is especially important when the technology is jointly developed or developed by others, such as by consultants, outside of a regular employment relationship. This is because IP rights in technology, materials, or other works are presumptively owned by the creators absent written assignment agreements (such as a consulting agreement or development agreement that includes a present assignment of IP rights) that spell out ownership rights. Just because you have paid someone to develop technology does not mean that you own the IP rights in the developed work. Again, there must be a present assignment of the IP rights from the developer to the payor. And even in a regular employment situation where the employer is presumed to own IP developed on the job, employment agreements that address ownership of IP rights in inventions and discoveries are still important in the event of disputes.

Consideration of the various forms of protection for IP rights in developed UAS-related technology is also important. Patents may protect the functionality or operation of new and non-obvious devices, systems, and processes. In the U.S., patents must be filed within one year of any public disclosure, use, or offer for sale of the technology sought to be patented – abroad patents must be filed before their subject matter becomes publicly known, used or offered for sale (there is no one-year grace period). Patents are a right to exclude others from

making, using, or selling the patented technology – they are not in and of themselves a right to commercialize one's own technology. The latter may be affected by the IP rights of others, such as earlier patents that bear on the technology. Thus, if one plans to expend significant resources in developing new technology, consideration of whether there are third-party patents that might block or inhibit commercialization (e.g., whether there is freedom to operate) is important. This is especially the case as UAS-related technology becomes a focus for commercial applications and there is a rush to patent such applications. The functionality of novel computer code or computer systems may be protectable by patent, as long as the innovation would not be considered to be merely an abstract idea implemented by standard computer parts. In the event broad patent protection is not available, aspects of the technology may be protectable by trade secret. In order for trade secret protection to apply, however, the subject matter to be protected must not be generally known or discernible – it must be kept and be able to be kept a secret.

Aspects of technology commonly considered for trade secret protection include source code or manufacturing processes. Thus, well developed trade secret policies are an important part of any UAS-related business. Copyright offers narrow protection of a particular expression such as in written documents, screen shots, or code, but does not protect the ideas or functionality exhibited in such works. Only patents or trade secrets can protect embodied ideas or functionalities. And trademarks, whether they be words, logos, slogans, and the like, protect the name or brand of products and services, acting as a source identifier for those products and services. Registration of copyrights and trademarks provides advantages and is relatively inexpensive, but registration is not required in order for the protections to apply.

Government contracting

In contracting with governments (U.S. or international) with respect to UAS systems, considerable attention must be paid to compliance obligations, intellectual property rights, and export (trade regulation) restrictions.

Unlike in the commercial marketplace, willful failure to comply with the terms of a government contract may lead to civil False Claims Act penalties, government-wide suspension or debarment, and even criminal liability. It is critical, therefore, that companies choosing to contract with the government understand the importance of assigning adequate resources to government-sponsored projects and having an adequate ethics and compliance function.

As to intellectual property, the U.S. government often obtains intellectual property rights by virtue of providing funding for technology development initiatives. Care must be taken in an emerging area such as UAS for a party not to inadvertently cede title or a royalty-free license to its intellectual property rights through these arrangements. Government contractors generally can retain title to patents conceived or first reduced to practice under a government contract, but the government customer receives a perpetual, non-exclusive right and license to authorize others to use the patent for government purposes. Likewise, the U.S. government typically receives unlimited rights in technical data first produced under a government contract. The government, however, may receive narrower rights when the intellectual property is developed under mixed funding. Contractors need to understand how these rules work and take steps to protect their rights, including by properly marking pre-existing technical data developed at private expense that will be used in the performance of a government contract.

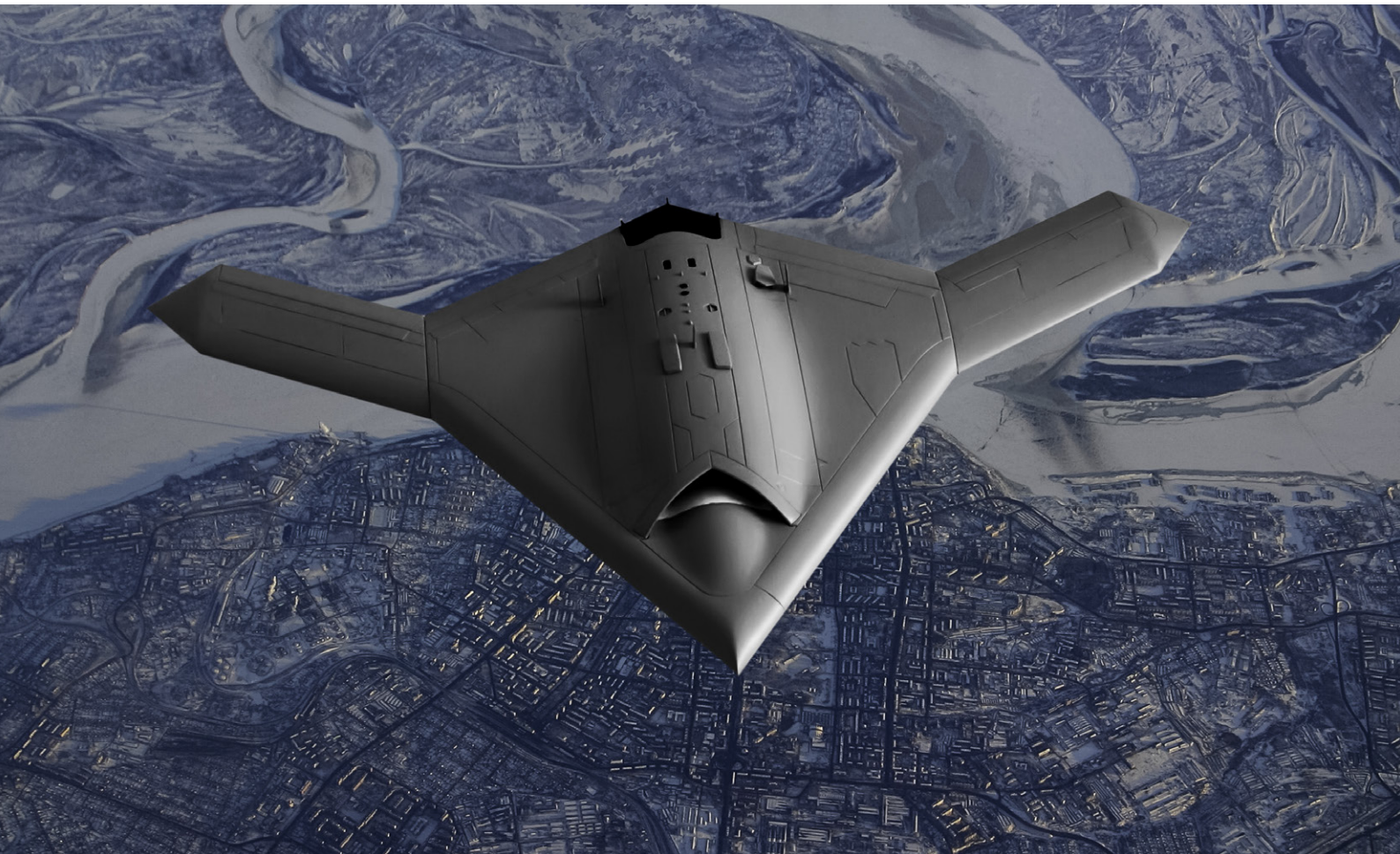
Although contracting with the government can increase risks, there also are some potential countervailing benefits, such as potential sovereign immunity-based defenses to third party tort lawsuits that may be available when the government participates in or approves the design of a UAS.

UAS or related equipment developed under contract with the U.S. military also may be subject to heightened export control restrictions (International Traffic in Arms Regulations).

Once developed and protections have begun, consideration of commercialization approaches, such as licensing, come to the fore. In addition to clarifying ownership and scope of permitted uses of the technology, licenses or similar agreements typically also address the remuneration or payments for permitted manufacture, use or sale of the technology, allocation of costs, contracting party representations and warranties concerning the technology, liability if the technology is found to be unsafe or infringing of others' IP rights, and indemnification if the technology causes harm to tangible or intangible rights of others. Particular attention must be paid to identifying the ongoing rights of each party to ownership, licensing, sublicensing, and usage of the IP rights in the subject technology as part of any contract, whether it be a commercial sale agreement, joint venture, or other acquisition. An IP originator may want to maintain full control, ownership, and patent filing, licensing and legal enforcement rights as to the background technology, foreground technology, enhancements and improvements, providing the counterparty only a limited license with restricted rights (if any) to sublicensing. Or, a counterparty who is developing an extensive system architecture around the originator's IP and funding the improvements and enhancements, may want to obtain significant (and potentially exclusive) rights to the IP rights in the counterparty's business area and have the right to control further licensing, transactions, patent filings, and legal actions to enforce patents as part of the commercial transaction. Thus, the IP terms of commercial agreements are likely to be heavily negotiated depending on the unique nature of the UAS offering and the enhancements being made to the system as part of the commercial development, purchase, licensing, joint venture, and/or sale agreement.

Privacy

Commercial use of UAS may prompt significant privacy concerns, as evidenced in the legislation presented in California. No less than five states – California, Idaho, North Carolina, Oregon, and Texas – already have



enacted laws that address UAS use by private entities. While the legal requirements vary, the California, Idaho, and North Carolina laws generally prohibit the capture of images from a UAS in a manner invasive to a person's privacy. The Oregon and Texas laws prohibit certain uses of UAS over private property. In February 2015, in the United States, President Obama issued an executive memorandum on privacy issues and government use of UAS and established a multistakeholder process led by the National Telecommunications and Information Administration (NTIA) to establish best practices.

In addition to these statutory restrictions, in the United States, common law-based protections for individual privacy should be factored into commercial plans to deploy UAS. A potential invasion of privacy claim is the tort of "intrusion upon seclusion," which has been adopted by most states. Under a common formulation of the tort, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." One who has established a cause of action for invasion of privacy is generally entitled to recover damages: for i) the harm to his interest in privacy resulting from the invasion; ii) his mental distress proved to have been suffered if it is of a kind that normally results from such an invasion; and iii) special damage of which the invasion is a legal cause.

The pursuit of such claims by individual plaintiffs, while in the past not particularly common, has very clear potential to expand in the case of UAS given the privacy concerns already expressed by certain constituencies, which are likely only to intensify as commercial UAS use becomes more common.

Outside of the United States, in almost all of the markets of interest to commercial users of UAS, governments have already enacted data protection laws of general applicability to business collection of personal data. Unless exemptions are made available by overriding regulation, businesses planning to deploy UAS in any European market, and multiple other jurisdictions in Asia and Latin America, would be advised to include data protection and privacy compliance in their regulatory planning as well.

The types of privacy and data security compliance actions likely to be required, whether in the United States, Europe, or other markets, will likely involve the provision of some form of external notice about the personal data gathered by the UAS and its contemplated uses, as well as the implementation of certain types of policies and procedures – such as data security and data retention policies – to manage such data. The UAS industry need not reinvent the wheel in designing such compliance programs; other industries' experience can provide valuable "lessons learned" and recognized industry standards for privacy and data security programs, and may provide useful (although not necessarily authoritative) roadmaps.

In addition to planning for compliance, commercial UAS users should plan to address privacy and data security risks in ongoing agreements (such as joint venture agreements). Parties to an agreement will need to determine whether the ability to oversee operations is a sufficient safeguard or whether additional rights are needed to ensure privacy issues are addressed. Specific warranties and representations should be included in purchase/sale transactions to ensure that the purchaser acknowledges its obligations to operate the UAS consistent with all legal requirements.

Consideration also should be given to the allocation of liability between the parties to the transaction (as well as contemplation of insurance as to the same) as to privacy and data security compliance.

Conclusion

As is the case of any new technology deployment, in contracting for UAS transactions, it is both critical to understand the shifting legal sands as well as to draw heavily upon previous "new industry" lessons in developing the contractual models for your UAS contracts. Both the "known" and "unknown" must be anticipated, and care must be taken in considering as many possible outcomes and variables as possible to best protect your position in these transactions.

The authors would like to recognize the contributions made to this article by Jared Bomberg, Thomas Connally, Celine Crowson, Tazewell Ellett, Nathaniel Gallon, Trey Hanbury, Robert Kyle, Christian Mammen, Thomas McGovern, Harriet Pearson, Patrick Rizzi, Andrew Spielman, Timothy Tobin, Niki Tuttle, and Erin Weber.

Steve Kaufman
Partner, Washington, D.C.
T +1 202 637 5736
steven.kaufman@hoganlovells.com

Randy Segal
Partner, Northern VA
T +1 703 610 6237
randy.segal@hoganlovells.com

Notes

www.hoganlovells.com

Hogan Lovells has offices in:

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest*
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Jeddah*
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Philadelphia
Rio de Janeiro
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Tokyo
Ulaanbaatar
Warsaw
Washington, DC
Zagreb*

* Associated offices