10th Edition

Global Intellectual Property Newsletter

A topic for 2016 – Digitalisation 4.0

Issue 06/16

CLIFFORD
CHANCE

contents

10th Edition

Welcome to the **10th edition** of our **Global IP Newsletter**. We look forward to updating you on current trends and developments in the world of intellectual property law in Europe and across the globe.

In this **June issue**, our main topic will be "**Digitalisation 4.0**", encompassing the progressive influence of computerised systems and applications on our private and professional lives, and its many consequences for IP and other areas of law.

We will start with an analysis of the state of the European Database Directive adopted in 1996, evaluating the Directive's attempt to create a harmonised framework for providing IP protection for data in Europe in the light of the current technological developments (Big Data, Internet of Things).

We will also discuss the ramifications of data protection for employment law and whether dynamic internet protocol addresses can be considered "personal data". Data protection and the need for cyber security, as well as the protection of companies against cyber-crime, are topics raised in this issue.

This newsletter also covers Standard Essential Patents ("SEP"). In order to allow competitors to comply with technical standards, patent owners of SEPs are obliged to license them to competitors on fair, reasonable and non discriminatory (FRAND) terms. In this context, the Court of Justice of the European Union in *Huawei Technologies v. ZTE* recently set specific guidelines regarding the negotiations of such terms between the parties.

Further topics include 3D-printing and how it provides a unique way to bring digital creations to the physical world, but also poses substantial risks for the infringement of IP-rights.

With regard to marketability of digital products, consumer protection and antitrust law, this edition will cover not only the applicability of the rule of exhaustion on digital media, but also the current proposal for a directive on contracts for the online and other distance sales of goods, as part of the EU's "Digital Single Market" strategy, as well as the disputed practice of "geo-blocking" online content.

Finally, we examine the effect of the easing of the Iran sanctions on business deals.

We hope you enjoy this edition of the newsletter and look forward to receiving your feedback.

London: Rights in data in a Big Data/Internet of Things world – a new European consensus, or a step backwards?

In an increasingly interconnected world, with increasingly powerful computational and modelling tools, our ability to gather and process large volumes of data about an ever-increasing range of things is growing exponentially.

On one view, data is information, which should be free for use unless this conflicts with other interests recognised in law, such as privacy for personal data, trade secrets, or security. The ability to access and mine data for a wide range of purposes brings enormous potential public benefits.

On another view, building quality data collections requires investment and there is countervailing public benefit in granting economic incentives for those who make this investment to benefit financially from permitting third party use of the data they have collected. Ability to monetise data collections could provide much-needed revenue streams for educational and research establishments. It could also encourage investment in ensuring the data is of high quality and accuracy.

The Database Directive, Dir 96/9/EC, attempted to create a harmonised framework for providing intellectual property protection for data in Europe. The framework it created, as interpreted by the Court of Justice of the European Union, is widely seen to be inadequate, and it is now likely to be scrapped or substantially reformed. Debate is re-opening about whether the only means of control organisations who collect data should have over use of that data is the ability to choose to whom they give access, and on what terms, or whether free flow of data is more likely to be achieved if they have some form of intellectual property rights, subject to antitrust scrutiny in cases of abuse of dominant position.

Copyright protection under the Database Directive

In 1996, the Database Directive attempted to create a harmonised European model for protection of databases (defined as *"a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means").*

The Directive confirmed that original "selection or arrangement" of the contents of a database would be protected by copyright, where "originality" is judged by the question whether they constitute the "author's own intellectual creation", a test which has since been judicially applied across the field of copyright generally (*Infopaq* (Case C-604/10)). Protection for original selection or arrangement does not protect the contents, as such, although the Directive acknowledges that the contents of a database may in some cases be copyright works in their own right – the example often given is an anthology of poems.

Originality of selection or arrangement is unlikely to apply to collections of data from – for example – sensing or monitoring which are structured in a standard, logical manner.

Key Issues

- There are conflicting views on the value of IP protection for data.
- The Database Directive is widely seen as striking the wrong balance in this area.
- Subsequent judicial developments have highlighted the need for a change in approach.
- The EU Commission plans to provide for the "free flow of data", but what this will mean is unclear.
- Simply weakening IP protection for data may have adverse consequences, deterring investment and innovation and ultimately damaging data owners' willingness to share.
- Abandoning the EU's harmonisation initiative in this area, with nothing to replace it, is unlikely to improve the situation.

Quick Update

On 27 May 2016, the European Parliament and the Council anonymously adopted the EU Trade Secret Directive. As we reported in our 9th edition of this Newsletter, the new directive provides for a legal framework to harmonise the differing approaches taken by EU Member States to the protection of trade secrets in respect to the causes of action and remedies available. In particular, the directive also strengthens the right to freedom of expression and information, providing for adequate protection of investigative-journalists and "whistle-blowers". The EU Member States will have two years to implement the EU Trade Secret Directive into their national law.

Moreover, even if the data is not structured in a standard, logical manner, can copyright protection arise in the absence of a human author? Say, for example, a satellite is gathering meteorological data and sending it back to earth-based computers for automated analysis and presentation in various graphical forms. Who is the author whose intellectual creation is to be considered?

The UK Copyright, Designs and Patents Act 1988 attempted to deal with this issue by providing in s. 9(3) that *"In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken"* (*"computer-generated"* being defined as a work being generated by a computer in circumstances such that there is no human author of the work). However, this is UK domestic law only, which is not well explored in case law, and there is no harmonised European answer to this question.

Copyright protection for original selection and arrangement under the Database Directive now reflects international copyright law, namely Article 2(5) of the Berne Convention and Article 5 of the WIPO Copyright Treaty.

Sui generis protection under the Database Directive

The Directive also created a new sui generis right, often referred to as the "database right". This database right is available to EU "makers" of databases only. It protects substantial investment in the obtaining, verification or presentation of the contents of a database against unauthorised extraction or re-utilisation. "Makers" are defined (recital 41) as the person (which may be a company or other organisation) who "takes the initiative and risk of investing", as opposed to mere subcontractors. There is no originality requirement nor any legal test that depends on an author. There is an exception for non-commercial scientific research, among other things, but no general "data-mining right".

Subsequent cases in the Court of Justice of the European Union, in particular *William Hill v. BHB* (Case C-203/02), limited what was originally understood to be the scope of this right in cases where the "maker" of the data had created the data as a spin-off from other activities. The data in that case was data about sporting fixtures (i.e. who was competing, where and when) and had been compiled by the organisers of the sporting events. Potentially, however, this could just as easily be applied to someone who creates datasets about performance of – say – jet engines as part of remote monitoring and servicing them.

In December 2005, the Commission published its first evaluation of the Database Directive. It noted that the case for the sui generis right was unproven, and that its scope had been curtailed through decisions of the Court, but did not go as far as recommending repeal. This reflected the mixed opinions from respondents to the consultation, some of whom favoured repeal, while others favoured retention or modification.

The future of the Directive

In its December 2015 Committee Report "Towards a Digital Single Market", the European Parliament noted that the Commission's evaluation of the Database Directive considers it to be an impediment to the development of a European data-driven economy. The Committee on Industry, Research and Energy and Committee on the Internal Market and Consumer Protection both called on the Commission to follow-up on policy options to abolish the Directive.

The Commission has said its reforms will include "a European 'free flow of data' initiative that tackles restrictions on the free movement of data for reasons other than the protection of personal data within the EU". This raises a number of questions. Critically, could steps to facilitate free movement of data by removing intellectual property protection that may presently be available actually disincentivise people from investing in making high quality and useful data collections, or from sharing data when they do collect it? Moreover, the Commission must avoid a return to the pre-1996 diversity in how and whether data is protected across the EU, which will also not promote "free flow of data".

To achieve the Commission's stated objectives a nuanced approach will be required, taking account of the competing public interests, and ensuring a standardised approach across the European Union.

Congratulations to our London Team!

Vanessa Marsland was recently listed on Managing IPs list of "The Top 250 Women in IP 2016". She was also ranked as a "Trademark star" on Managing IP's list of IP Stars 2016.

Chambers and Partners, Intellectual Property – **Band 3**

"Vanessa Marsland of Clifford Chance LLP is best known for her handling of contentious matters, especially copyright, licensing and trade mark disputes. A source describes her as "one of the brainiest solicitors in London"."

Link Directory

1. The Database Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML
2. *Infopaq* (Case C-604/10): http://curia.europa.eu/juris/celex.jsf?celex=62008CJ0005&lang1=en&type=TXT&ancre=
3. UK Copyright, Designs and Patents Act 1988: http://www.legislation.gov.uk/ukpga/1988/48/contents
4. The Berne Convention for the Protection of Literary and Artistic Works: http://www.wipo.int/treaties/en/text.jsp?file_id=283698
5. The WIPO Copyright Treaty: http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295166
6. *William Hill v. BHB* (Case C-203/02): http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62002CJ0203&from=EN
7. European Commission's 2005 evaluation of the Database Directive: http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf
8. European Parliament's 2015 Committee Report "Towards a Digital Single Market": http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0371+0+DOC+XML+V0//EN

Frankfurt: Reducing risks in the digital workplace – labour law aspects

The use of digital media has taken over workspaces, bringing about new challenges for the protection of business secrets, know-how and personal data against unwanted disclosure. HR documentation and processes, due to split responsibilities, matrix structures and fears of having to involve employee representative bodies in any changes to HR matters, often are not accompanied by necessary legal safeguards. In this article, attention is drawn to some options to mitigate risks for business secrets and know-how through minor adjustments to HR documentation and processes.

Review of standard contract templates:

Standard contract templates should be reviewed and amended on a regular basis to follow technical developments. When making such amendments, implementing the following safeguards could be considered:

Confidentiality clauses:

- "Business secrets" have been defined by the labour courts, but in practice it is often difficult to demonstrate that certain information meets this definition. Standard contract clauses should therefore contain an obligation to also keep confidential "any information the employer has stated to be confidential". Email footers for internal use containing this statement may help extend the scope of protection.
- The protection of the business secrets of an employer, under a duty of good faith, does not automatically extend to business secrets of the parent or group of the employer. While most new standard clauses in the industrial sector contain this extension, older contracts often do not. Confidentiality clauses should be expressly extended to the benefit of the group of companies the employer belongs to.
- It is not entirely clear to what extent confidentiality obligations continue to apply post-termination – unless this is expressly set out in the contract.

Clauses on the return of company property:

Clauses on the return of Company property are often very detailed in Germany in order to meet the strict requirements of the standard contract terms test applied when testing whether any clause is enforceable to the detriment of the employee. Accordingly, many standard contracts contain a detailed list of IT items to be returned. However, the lists are often outdated. While this does not mean the employer cannot claim back other property, this often entails additional effort and costs which can easily be avoided. Such clauses should therefore be regularly adjusted for technical developments for new hires, and a "catch all" clause with regard to "any other" items received by the employer for the purpose of the employment relationship or in its context be added. The documents signed by employees relating to the return of company property, which are commonly part of the exit procedure, should be amended accordingly on a regular basis.

Older clauses on the return of company property often state that an employee must delete all copies of company documents/data from his personal IT at the time of exit. While IT policies may provide instructions as to where data must be stored so as to ensure that they remain available despite the employee erasing them on his personal IT means, we have seen cases where this was either not the case or the instructions were not followed in practice. Contractual clauses on the return of company property should therefore be changed in such way that they provide for the erasure of data only upon the request of the employer.

Review social media training:

While employees may sign declarations on data confidentiality and receive teaching on the legal consequences of breaching data secrecy, they may not apply this knowledge when it comes to their daily routine. The risks involved with

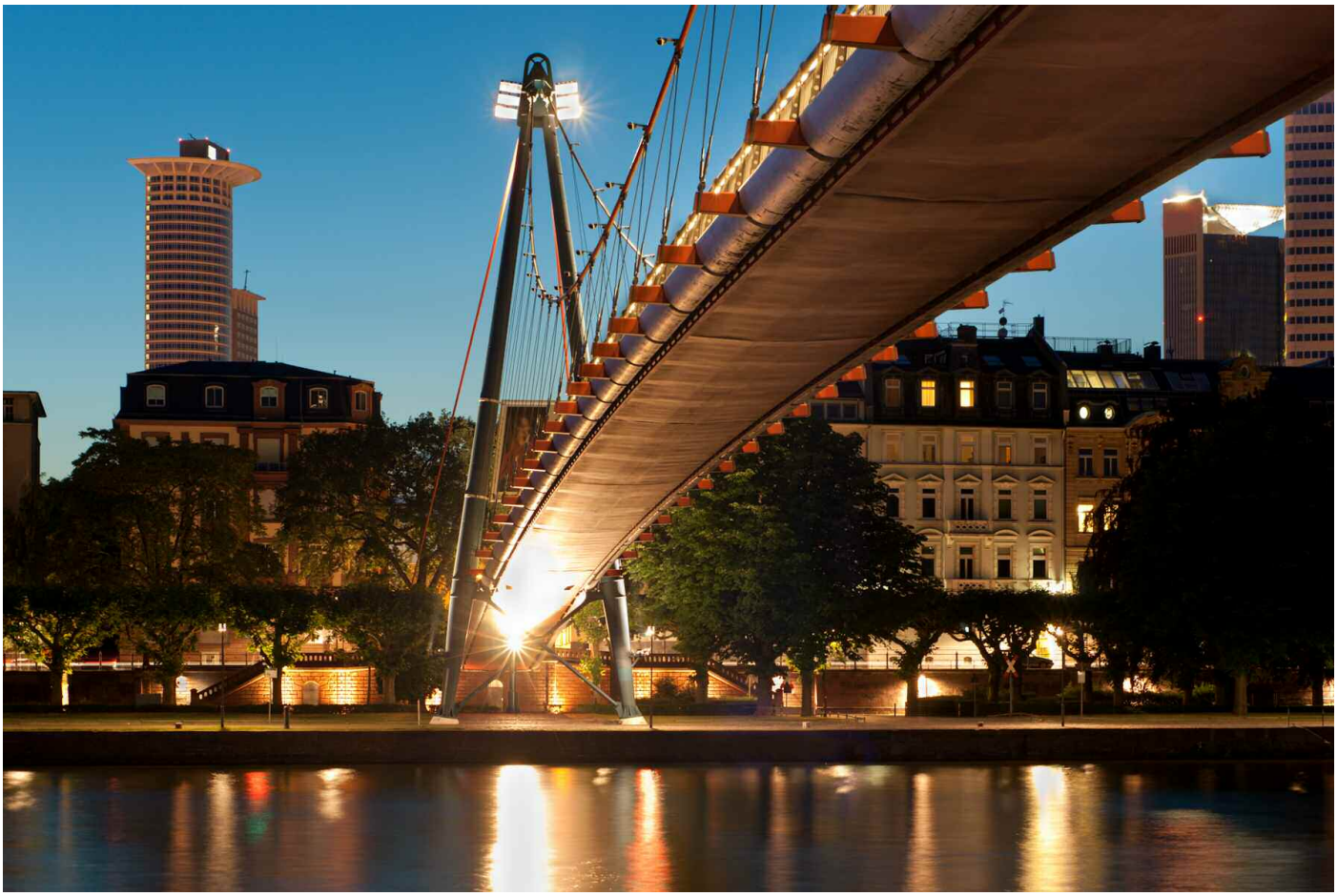
Congratulations to our German Team!

The team is named by Chambers Europe Guide 2016 in the category "Intellectual Property: Patent Litigation" and **Claudia Milbradt** is one of the ranked lawyers.

respect to the camera function of the smart phones employees bring to work were illustrated in an unfair dismissal case widely discussed in Germany (Higher Labour Court of Berlin, 17 Sa 2200/13, ruling dated 11 April 2014). A nurse in an intensive care unit had, over a long period of time, taken medical care of a baby and had posted pictures of the baby on Facebook, visible to a vast group of "friends". While the employing hospital had formally done everything correctly, handing out all the necessary leaflets and having the nurse sign confidentiality agreements, she simply did not draw a connection between those leaflets and the photos she posted on Facebook. She deemed the use of her photos and Facebook her personal affair. The dismissal issued by the hospital was declared unfair by the court. The court rated the employee's interest in continued employment higher than the employer's interest in terminating it in the specific circumstances. More importantly, however, damage with regard to reputation and loss of trust of patients had already been incurred. While most companies have long had social media and Bring-Your-Own-Device policies, it should also be ensured that sufficient training is also given with regard to the use of social media and smart phones in the workplace.

Review of an employee's exit procedure:

The documents employees sign as part of their exit from a company should also be drafted in such a way as to mitigate risks which arise where the employee's company email account is later accessed by the employer. It is advisable to include in such documents the return of company email accounts, an employee certification that no personal emails are included in the returned account and consent for the company to access the email account.



Amsterdam: Advocate-General opinion – Dynamic IP addresses to be considered personal data

The Advocate-General of the European Court of Justice opined on 12 May 2016 that dynamic IP addresses should be considered personal data as defined in Article 2 of the EC Data Protection Directive 95/46/EC if a third party (in this case an internet access provider) has access to additional information that would enable the identification of the internet user. If the opinion of the Advocate-General is followed by the ECJ, website providers collecting and storing dynamic IP addresses may come under close scrutiny from local data protection authorities in the EU.

Dynamic IP address

In short, an internet protocol ("**IP**") address is a unique numerical tag allocated to an information technology device (such as a computer or a smartphone) connected to the internet. An IP address enables such a device to identify itself and communicate with other devices. A distinction can be made between static and dynamic IP addresses. A static IP address is assigned permanently whereas a dynamic IP address assigns a different IP address each time a connection is made to the internet. In general most IP addresses are dynamic IP addresses. Website providers often collect and store information tied to IP addresses for marketing and website optimisation purposes.

Background

The main question in this case is whether the Federal Republic of Germany may collect and store the dynamic IP addresses of visitors to its websites. The background of the case is a dispute between a German politician and data protection activist, Patrick Breyer, and the Federal Republic of Germany. Breyer had lodged a request for an order against the Federal Republic of Germany to stop collecting and storing the dynamic IP addresses of the visitors of German governmental websites beyond the term required to enable the use of the website. In its defence the Federal Republic of Germany argued that such information is recorded and stored in order to protect itself against cyber attacks and also enable the identification and prosecution of such cyber attackers. Pursuant to Breyer's line of reasoning, the IP addresses can be traced back to individual persons and therefore constitute personal data. Breyer's claim was dismissed by the district court, but in appeal the court decided to partially award his claim and ordered the Federal Republic of Germany to stop storing dynamic IP addresses if the visitor had disclosed his e-mail address and the storage was not required in order to enable the use of the website.
The German Federal Supreme Court then referred questions to the ECJ for a preliminary ruling.

Opinion of Advocate-General Campos Sánches-Bordona

The fundamental question in this case is whether an IP address stored, in connection with a visit to a website, will constitute personal data (under the EC Data Protection Directive 95/46/EC) if a third party has additional data which will make it possible to identify the individual.

In answering this question the Advocate-General first noted that the question whether a dynamic IP address can be considered personal data has been the subject of heavy debate for quite some time. In determining whether a person is identifiable *'account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person'.*
The Advocate-General is of the opinion that the submission of a request to an internet service provider by a website provider for such additional information can be considered to be a "*means reasonably likely to be used'* and therefore dynamic IP addresses constitute personal data.

Key Issues

- Advocate-General of the ECJ opines that dynamic IP addresses constitute personal data.
- ECJ to give final decision. If the Advocate-General view is followed, website providers processing dynamic IP addresses will need to comply with Data Protection Directive requirements.

The Advocate General of the CJEU stated that if dynamic IP addresses were not regarded as personal data from the point of view of the provider of an internet service, they could retain them indefinitely and at any time ask the internet provider for additional data in order to combine them with the dynamic IP address and accordingly identify the internet user.

Implications

The ECJ is due to render its final decision, however it is likely that the Advocate General's opinion will be followed. Should the ECJ decide to follow the Advocate-General's opinion this could have serious implications for website providers as any recording, storage or use of dynamic IP addresses after the website visit would require consent from the website user. Any processing of dynamic IP addresses would then need to comply with the requirements as laid down in the EC Data Protection Directive 95/46/EC. In accordance with the directive, website providers would be entitled to record, store or use dynamic IP addresses without consent if they can substantiate that such processing is required to ensure the proper functioning of the website (and as such have a legitimate interest that prevails over the privacy interests of the website user).

Frankfurt: Cyber security and cyber crime – new challenges for companies in light of a changing legal landscape

Currently, the legal landscape regarding cyber security is changing, both on a German and European level. In Germany, the new law regarding the Improvement of the Security of Information Technology Systems ("**IT Security Act**") obliges certain operators of critical infrastructures to implement a minimum standard regarding cyber security and to report material incidents. On a European level, a new EU Directive on Network and Information Security ("**EU NIS Directive**") will be adopted this year in order to achieve a high common level of security for network and information systems within the EU.

Cyber crime – threat level and potential consequences

Companies are subject to cyber attacks twenty-four hours a day, seven days a week. Most of the time, companies do not even notice the attacks. In recent years, the threat of cyber attacks has increased. For instance, the number of malware designed for Windows quadrupled between 2012 and 2015. Concurrently, more and more services and production workflows are driven via the internet and employees can access confidential business data outside the office via notebooks or smartphones, thereby creating new points of attack for cyber criminals. The various types of cyber crime are manifold and include simple spam emails containing malware, denial-of-service-attacks disconnecting entire IT systems in order to extort the affected company, and social engineering, which involves getting individuals to disclose confidential information through deception (for example phishing or fraud). Furthermore, in industrial espionage, confidential information is frequently accessed by persistent advanced threats accessing entire IT systems to implement key loggers which record each key pressed by the user and the programs used.

Such cyber security incidents may have severe financial impacts on affected companies as they can lead to, amongst others, patent violations, the loss of competitive advantages due to loss of business secrets, compensation payments, loss of production and high costs caused by measures necessary for resolving incidents. The annual financial impacts of cyber incidents for the German economy are estimated at EUR 51 billion.

Furthermore, the reputational impacts of such incidents can be devastating as they usually attract media attention. If companies depend on their customers' trust in absolute confidentiality of their information, data loss may even wipe out the companies' existence.

German IT Security Act

In Germany, certain companies face new statutory obligations regarding cyber security. In view of the increasing threat level, the German legislator adopted the IT Security Act in July 2015 in order to give special protection to operations of particular importance to the community. The IT Security Act obliges certain operators of critical infrastructure in certain sectors to implement appropriate and state of the art technical and organisational measures to mitigate the risk of incidents affecting their IT systems. The operators also have to regularly prove the implementation of such measures through audits and certifications. Furthermore, operators are obliged to report significant IT incidents to the Federal Office for Information Security immediately. The types of operations within the scope of the IT Security Act are considered in a May 2016 regulation by

Key Issues

- Cyber security incidents may have severe financial and reputational consequences for companies.
- Under the new German IT Security Act, operators of critical infrastructures are obliged to implement effective IT security measures and report incidents.
- On an EU level, a Directive on network and information security is on the way, providing for transnational cooperation to mitigate cyber security risks and establishing IT security and notification requirements for operators of essential services and digital service providers.

the German Federal Ministry of the Interior. However, the regulation only provides the parameters for assessing whether an operation can be considered critical infrastructure. Therefore, operators themselves must assess whether they fall within the scope of the IT Security Act and have to fulfil the duties provided therein.

This is of particular relevance as violations of duties under the IT Security Act can lead to administrative fines of up to EUR 100,000 for each case, including cases of negligence. Such administrative fines are primarily imposed on individuals. However, if managers violate duties under the IT Security Act or violate related supervisory duties, administrative fines may also be imposed on the company they are acting for.

The current regulation only relates to the energy, water, food and IT and telecommunication sectors but it is intended to regulate the remaining sectors (transport, healthcare, financial markets and insurance) by the beginning of 2017.

EU NIS Directive

Against the background that cyber security incidents have transnational impacts and affect data hosted across various jurisdictions, the EU will likely adopt the EU NIS Directive by August 2016. According to the current draft, the EU NIS Directive provides for EU-wide cooperation in order to face cyber security risks. In particular, a Cooperation Group facilitating strategic cooperation and the exchange of information among member states and a Computer Security Incident Response Team network promoting swift operational cooperation in cases of cyber security incidents shall be created. Furthermore, similar to the IT Security Act, IT security and notification requirements for operators of essential services and for digital service providers shall be established. However, in this regard, the proposed provisions of the EU NIS Directive partially go beyond the IT Security Act as they relate to a wider scope of obliged operators, including online marketplaces, online search engines and cloud computing services. Once adopted, the EU NIS Directive will have to be transposed by the member states within 21 months. In Germany, this will most probably lead to amendments to the recent changes implemented by the IT Security Act. Therefore, the developments on the legal landscape regarding cyber security are not yet finalised, neither on a German nor European level.

New challenges for companies

In view of the changes on a German and EU level, companies face new challenges with respect to IT compliance. In particular, they have to assess whether they fall within the scope of the IT Security Act and whether they have to fulfil the corresponding obligations. Furthermore, companies are advised to follow legal developments to prepare themselves for further changes, such as the EU NIS Directive.

However, even if companies do not fall within the scope of the IT Security Act and the EU NIS Directive, cyber security issues should be addressed by implementing a comprehensive information security compliance management system in order to protect against reputational damages, financial losses and further consequences associated with cyber security attacks. This system requires a risk assessment of the entire company, not only in regards to technological aspects. Concrete cyber security measures should be implemented and a robust cyber disaster response plan addressing reputational risks and legal obligations should be developed. Furthermore, relevant policies on data collection, confidentiality and IT, should be reviewed and amended in view of the implemented and proposed changes.

Brief description to be included into the table of contents:

Deficient cyber security and information protection bear considerable risks, particularly for the protection of business secrets and IP rights. Furthermore, the legal landscape regarding cyber security is changing both on a German and European level, presenting new obligations and challenges for companies.

London/Brussels: Standards Essential Patents in Europe – current status

Certain fields of technology require manufacturers to operate to technical standards in order to ensure interoperability of devices, data and/or networks.

These same fields are typically the subject of many patents owned by many different organisations. Any one of them might be able to prevent others from producing devices working to the standard by refusal to license or could use their patent leverage to demand disproportionately high royalties.

The practice has therefore grown up of encouraging market participants to engage in the standards setting process, to declare where they have patents that may read on to the standard to enable participants in the process to make informed choices between standards, and to agree to license their patents on FRAND or RAND terms, i.e. (fair), reasonable and non discriminatory.

Congratulations to our Belgium Team!

The team is ranked in Chambers Europe 2016 in the category 'Competition/European Law'.

Notable practitioners
"Chairman of the firm's global antitrust group **Thomas Vinje** acts on competition and IP mandates. He is advising FairSearch Europe, an industry body with members such as Nokia, Oracle, Microsoft, Expedia and TripAdvisor, on the EC investigation into Google's alleged abuse of dominance in the online search market. Sources enthuse that "he is brilliant, an incredible communicator."

Work highlights
"Acted for Samsung Electronics on a EC investigation into alleged abuse of dominance related to standard-essential patents."

This deceptively simple proposition raises a number of issues in practice. The European Commission has published detailed guidance for standards-setting bodies in its 2011 Guidelines on Horizontal Cooperation Agreements, as well as pursuing antitrust investigations under (what is now) Article 102 of the Treaty on the Functioning of the European Union ("TFEU") for alleged abuse of dominance.

Failure to declare patents reading on to a standard – "patent ambush"

On 30 July 2007, the Commission sent Rambus a Statement of Objections, setting out its preliminary view that Rambus may have infringed (what is now) Article 102 of the Treaty on the Functioning of the European Union ("TFEU") by abusing a dominant position in the market for DRAMs. In particular, the Commission was concerned that Rambus intentionally concealed that it had patents and patent applications which were relevant to technology used in the DRAM standard set by US-based standard setting organisation JEDEC, and then subsequently claimed royalties for those patents. The case was ultimately resolved by Rambus giving commitments. These commitments enabled DRAM manufacturers to sign a bundled licence for the use of Rambus' technologies incorporated in the JEDEC standards at lower rates than Rambus had been demanding.

Key Issues

- A key objective in this area has been to obligate patent holders to disclose relevant patents that during the standard-setting process and to license essential patents on a fair, reasonable and non discriminatory basis.
- While the system should encourage licensing of standards essential patents, it also requires would-be licensees to play fair and patent holders to be able to enforce their rights if they do not.
- The inherent uncertainty around patent scope and validity complicates the picture, as there may be genuine disagreements about patent validity and whether patents do or do not cover implementation of a given standard.

Of course, the question whether any patents in a large portfolio could read on to a standard is not always straightforward and non-disclosure may not be intentional concealment. Expert views may legitimately differ on patent scope. How standards are implemented may also evolve. The Commission's 2011 Horizontal Guidelines require standards-setting organisations to have good faith disclosure policies but do not go so far as prohibiting any enforcement of patents that, in good faith, were not disclosed.

What happens when the parties cannot or will not agree FRAND terms?

(i) Samsung and Motorola

After trying, but failing, to reach agreement on FRAND terms, in April 2011, Samsung started to seek injunctions against Apple on the basis of its standards essential patents relating to the European Telecommunications Standardisation Institute's (ETSI) 3G UMTS standard, a key industry standard for mobile and wireless communications. In December 2012, the Commission informed Samsung of its preliminary view that it considered Apple a willing licensee on FRAND terms for Samsung's standards essential patents and that consequently, the seeking of injunctions against Apple in several Member States might constitute an abuse of a dominant position in breach of Article 102 TFEU.

These proceedings were ultimately resolved by Samsung giving commitments not to seek any injunctions in the European Economic Area on the basis of any of its standards essential patents, present and future, that relate to technologies implemented in smartphones and tablets against any company that agrees to a particular framework for licensing the relevant patents. Parallel proceedings by the Commission against Motorola, meanwhile, ended up with an infringement decision against Motorola, albeit with no fine.

The Samsung licensing framework provides for:

i. a negotiation period of up to 12 months; and

ii. if no agreement is reached, a third party determination of FRAND terms by a court or by an arbitrator if both parties agree to arbitration.

This approach does not rule out the possibility of seeking injunctions where a licensee refuses to engage in negotiations or in other exceptional circumstances. However, since there may be a willingness to negotiate, but difficulty in agreeing FRAND terms, it also provides a framework within which any differences in opinion about standards-essentiality or validity of the patents, or royalty rate and royalty basis can be resolved, if necessary with the assistance of court or an arbitrator. The commitments leave a potential licensee free to argue that the relevant patents are invalid or not infringed without being deemed unwilling.

Given that there are frequently disagreements between reasonable parties about patents scope, and given the patent ambush concerns, it is not surprising that disclosures against standards include patents that, when tested before a court, are held not to be infringed by operating to the standard.

Additionally, many patents are found invalid when tested, even if they do appear to read on to the standards. These should be discounted when assessing the royalty entitlement of the patent owner. The Commission has recognised this, and has in the past allowed negotiations to proceed on the basis of "proud lists" of a subset of the total portfolio.

Congratulations to our Asian team!

The team was recently ranked in different directories, e.g.:

- Managing IP, Copyright: China – **Band 2**
- Legal 500, Intellectual Property: Hong Kong – **Band 2**
- Chambers, Intellectual Property: China – **Band 3**

(ii) Huawei v ZTE

In July 2015 the Court of Justice of the European Union handed down its decision in *Huawei Technologies v. ZTE* (Case C-170/13), which concerned the LTE standards. The case was a reference from the German courts, which had developed their own ("Orange Book") approach to the issue of injunctive relief in standards essential patents and wished to test its compatibility with EU competition law.

The Court's decision provides guidance for how both patentee and implementer must behave. It provides that a standards essential patent holder does not abuse its dominant position if it goes to court if:

1. prior to bringing an action, the proprietor has, first, alerted the alleged infringer of the infringement complained about by designating that patent and specifying the way in which it has been infringed;
2. after [i.e. "if"] the alleged infringer has expressed its willingness to conclude a licensing agreement on FRAND terms, the patent holder has presented to that infringer a specific, written offer for a licence on such terms, specifying, in particular, the royalty and the way in which it is to be calculated; and
3. where the alleged infringer continues to use the patent in question, the alleged infringer has not diligently responded to that offer, in accordance with recognised commercial practices in the field and in good faith, this being a matter which must be established on the basis of objective factors and which implies, in particular, that there are no delaying tactics.

This guidance will help in simple cases where, for example, an alleged infringer fails to engage in good faith. Open questions remain. These include: what will

be FRAND terms in any specific case (i.e. not just rate but also basis of calculation and licence terms, as well as patent validity and standards essentiality); how to approach royalty assessment where a patent holder owns multiple patents relating to the standard; whether standards essential patent holders whose patents cover components can legitimately select at which point in the value chain they grant licences; as well as more procedural issues about e.g. impact of the patent holder's offer not being found to be FRAND.

(iii) Other Pending Cases

The German and English courts have been exploring some of these issues since the Court's judgment in *Huawei v. ZTE*. In *Sisvel v. Haier* (Case I-15 U 65/15) the Higher Regional Court of Dusseldorf determined in January 2016 that the court below erred in not considering whether the patent holder's offer was on FRAND terms before granting an injunction. In *St. Lawrence v. Deutsche Telekom* (Case 6 U 44/15), in April 2015, the Higher Regional Court of Karlsruhe stayed an injunction previously granted by the lower court in circumstances where the patent holder had secured an injunction against network operator Deutsche Telekom, whereas its normal practice had been to license to intervening device manufacturers, and relevant device manufacturers had indicated willingness to take licences. Both cases are currently under appeal.

Meanwhile in London, the case *Unwired Planet v Huawei and Samsung* [2015] EWHC 1029 (Pat) is proceeding through multiple phases and hearings as the court resolves a series of issues surrounding validity, standards-essentiality, and whether the licence offered by the patent holder was on FRAND terms.

Continued focus on standards setting by the European Commission

As part of its wide-ranging Digital Single Market initiatives, on 19 April, 2016 the European Commission published a Communication on ICT Standardisation Priorities for the Digital Single Market (COM (2016) 176 final). The Communication says that standardisation requires a balanced IPR policy based on FRAND licensing terms. It advocates a fast, predictable, efficient and globally acceptable licensing approach, which ensures a fair return on investment for standards essential patent holders and fair access to standards essential patents for all players. Further developments in this area are expected over the forthcoming months.

Link Directory

1. Commission's 2011 Horizontal Guidelines: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52011XC0114(04)
2. Commission Confirmation of Rambus Statement of Objections: http://europa.eu/rapid/press-release_MEMO-07-330_en.htm?locale=en
3. Commission Decision following Rambus Commitments: http://ec.europa.eu/competition/antitrust/cases/dec_docs/38636/38636_1203_1.pdf
4. Commission Statement on Samsung Statement of Objections: http://europa.eu/rapid/press-release_IP-12-1448_en.htm
5. Samsung's Commitments: http://ec.europa.eu/competition/antitrust/cases/dec_docs/39939/39939_1502_5.pdf
6. Commission's Motorola Decision: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014XC1002(01)&from=EN
7. IEEE Updated IPR Policy: http://standards.ieee.org/develop/policies/bylaws/sect6-7.html
8. *Huawei v. ZTE* (Case C-170/13): http://curia.europa.eu/juris/liste.jsf?num=C-170/13
9. *Unwired Planet v Huawei and Samsung* [2015] EWHC 1029 (Pat) eplaw.org/wp-content/uploads/2016/05/UK-Unwired-Planet-CAT-transfer.doc
10. *Sisvel v. Haier* (Case I-15 U 65/15): http://openjur.de/u/876177.html
11. *St. Lawrence v. Deutsche Telekom* (Case 6 U 44/15): http://openjur.de/u/776505.html)
12. Commission Communication on ICT Standardisation Priorities for the Digital Single Market: https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market

Milan: 3D-printing: An overview of intellectual property issues under Italian law

3D printers are forecast to do to the tangible world what the internet did to the intangible: large-scale circulation of information enabling the reproduction of objects, comparable to the internet and peer-to-peer distribution. Consumers will be able to take on a new role, reproducing objects found on the market.

Such progress can also engender conflicts, and a new, more subtle concept of infringement will be required, one that goes beyond the current Italian legislation and its case law interpretations. Otherwise, the law risks being ill-prepared for the new technologies.

Introduction

3D printing, also known as additive manufacturing (AM), consists of a number of different processes used to create a **three-dimensional object.**

In 3D printing, **successive layers** of material are formed using computer control. The objects can be almost any shape or geometry and are produced from a 3D model or other electronic data source.

This article addresses, among other issues:

(i) 3D printing and the law of patents and copyright;

(ii) 3D printing and the law of trademarks and design law; and

(iii) 3D printing and unfair competition principles.

3D printing and the laws of patent and copyright

Under Italian law, there is no infringement of a patent where the supposed infringing actions are carried out "***privately*** *and for* ***non-commercial*** *purposes*" (Article 68 of the Italian Intellectual Property Code).

Key Issues

- Outside of copyright law, consumers who print objects may have the opportunity utilise the exemption that allows use of a patent for private use or to argue that their use is not in the context of an economic activity or trade.
- Suppliers of 3D printers or of infringing files could be charged with contributory infringement doctrine. The concept is not part of a body of laws, but exists only in precedent judicial decisions and exclusively in relation to patents.
- Where suppliers of 3D printers have used disclaimers to set forth contractual provisions, they may have a valid defense, which would be evaluated on a case-by-case basis.
- Provisions governing unfair competition law offer more opportunity to stop infringement, especially in the presence of certain prerequisites.
- Much in this field remains unexplored, and identifying appropriate means of achieving redress for some forms of conduct may prove tricky.

Under the law of patents any act that is done in private and for non-commercial purposes is lawful. This stands in contrast to the Italian law on copyright, which is more restrictive and provides an exception only for some private uses (such as the making of backup copies for software or the private use for phonograms and videograms).

The principles that govern copyright law include Article 5(5) of the Copyright Directive 2001/29/EC, which states that the exceptions to copyright protection under Article 5(1) "*shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not* ***unreasonably prejudice*** *the legitimate interests of the rightholder*". While this was not carried over into the Italian legislation, it may nonetheless be taken into consideration by the courts.

Leading Italian academic authorities (such as Prof Cesare Galli) take the view that the Italian Intellectual Property Code must be interpreted in a manner

consistent with the Italian Constitution, which requires identical situations to be treated in the same way, and to apply the principle set forth in the copyright law as a statement of general principle. That means that, at the very least, anyone **who serially reproduces an object** that is subject to patent, or takes other action with the aim of evading the law of patents, will be acting in a manner that is **excessively prejudicial for the right-holde**r (as they would be under copyright law), and as a result, they should be considered to have committed an infringement.

This however is an interpretation that breaks new ground, and has yet to be considered by the courts.

Arguing that supplying the means (both the file that forms the basis for the reproduction, and the 3D printer itself) that enables such actions to be taken, would constitute infringement, even where the supply is to private individuals, looks less controversial, given the doctrine of contributory infringement.

The Italian legislation does not explicitly deal with **contributory infringement.**

The legal concept of contributory infringement may however be argued through interpretation of the existing law, and most academic authorities treat contributory infringement as an act that is not *per se* unlawful, but regulated by general principles of tort law.

The conditions for holding an act to be a contributory infringement of a patent should be that: (i) the means supplied by the contributory infringer are only suitable for committing a direct infringement of the intellectual property right; and

(ii) damages may be awarded only if the contributory infringer knew (or should have known) the purpose to which those means would be put.

More particularly, case law indicates that contributory infringement of a patent is apt to occur mainly in two cases:

(i) a third-party supplier provides the means (raw materials, components, equipment and even designs and know-how, *per* the Italian Supreme Court, Order No. 9,410 of 1 November 1994,) and these are **unequivocally intended** to be used in the exploitation of the patent; or

(ii) the raw materials or components are capable of being used for lawful purposes, but the supplier is **aware that the supplied materials will be used to infringe the paten**t (see Supreme Court, Order No. 5406 of 12 June 1996).

One possible solution would be to prepare disclaimers stating that the printers may be used only for lawful activities; or the inclusion of contractual obligations to a similar effect, in agreements with users. Naturally, the situation will have to be judged on a case-by-case basis. However, the disclaimers could be treated as ineffectual boilerplate and a futile defence against infringement.

3D printing and trademarks and design law

One of the most common applications of 3D printing is in making **spare parts**. Under Article 241 of the Intellectual Property Code, such reproductions are lawful in Italy provided only **design rights are contravened**.

The unauthorized duplication of 3D-printed designs not only raises patent and copyright issues but also threatens to undermine trademark, trade dress and design patent rights. Nonetheless, the difficulties encountered in registering shape trademarks within the European Community (on the basis that they lack the ability to have intrinsic distinctive character) are well-known. This means the hypothesis most commonly discussed is where the 3D-printed object carries the **trademarked name of the rightholder**.

In trademark and design law the prohibition is upon use in economic activity, even if there is no specific exemption for private use as there is in connection with patents.

It is conceivable that the concept of economic activity might be expanded, in particular with respect to fashion and luxury goods trademarks, where the consumer cooperates with the rightholder by making the marks visible, wearing them and displaying them, publicly. Such an interpretation may however be seen as a stretch.

By contrast with patents, there is no precedent in the Italian case law on trademarks and design that supports the notion of contributory infringement.

Nonetheless, there are no general grounds that would prevent it being argued on the basis that it should apply by analogy.

Unfair competition law

In addition to interpreting the principle stated by the Copyright Directive as being of general application, in Italy

some forms of conduct may constitute unfair competition.

While the general provision contained in Article 2598(3) of the Italian Civil Code would appear to impose a general prohibition upon acts of unfair competition, it rarely operates as such. The view that it operates as a general rule prohibiting unfair competition and misappropriation has only been favoured by a minority of the case law.

There are however two forms of conduct that the case law has identified as unlawful, and which may be applicable to 3D printing, namely:

(i) direct copying of another's work by pantographs, scanner or similar; and

(ii) copying of a whole series of products that are not standard within the sector in question.

Conclusions

Much in this field remains unexplored, and identifying appropriate means of achieving redress for some forms of conduct may prove tricky.

Careful consideration will be required if advancing technologies and information exchange are not to undermine the IP that drives much of the Italian economy, in particular fashion, luxury and design.

Paris: The copyright exhaustion rule: an outdated principle in the digital era?

In a digitalized world, the borders between Member States and the use of tangible media tend to disappear. This leads to new methods of distributing IP-protected material and raises the issue of how the rule of exhaustion is enforced.

The rule of exhaustion seeks to enforce the primary objectives of the European single market, namely (i) preventing the partitioning of the market by removing borders between EU Member States, and (ii) preventing the importation of products to the EU, whether or not they had been lawfully marketed in non-Member States. To that end, it provides that once a product incorporating an IP right has been marketed in a Member State with the right holder's consent, that right holder cannot prevent the product from being distributed in another Member State on the sole ground that the right holder did not agree to such a Member State distribution.[i] The reference made to the import operation means that it is applicable only within the EU, due to the reservation raised by the European Commission with respect to Article 4(d) of the TRIPS agreement.

Under European and French law, the exhaustion of copyright does not apply to works stored in a digital form, except where computer programs are concerned. This has led copyright holders to find alternative distribution methods.

Inapplicability of the rule of exhaustion in the digital world

Copyright exhaustion is typically a border to a copyright holder's right of distribution within the European single market as it implies that copyrighted works may only be distributed where tangible products are involved. However, the European Court of Justice has extended the rule of exhaustion to computer programs.

Key Issues

- The rule of exhaustion provides that once a product incorporating an intellectual property right has been marketed in a member State with the IP right's owner's consent, said owner may not prevent the same product from being distributed in another member State on the sole ground that it did not agree to such distribution in said other member State.
- French and European law, when using the notion of "products", designate tangible copies and thus, do not apply the rule of exhaustion to digitally-stored works.
- So far, French and European law has only recognized an exception for software downloads.
- However, owners' rights on digital works may be exhausted through the exercise of the right to communicate, according to which once the work has been communicated for the first time on a public website, anyone may use it on their own websites without needing to pay any additional royalty to the copyright holder.
- An alternative solution may be reached through cross-border licences. Directive 2014/26/EU of 26 February 2014 allows now collective management organizations to conclude cross-border licences with streaming companies, in order to give them access to a wider repertoire in consideration of a remuneration to the copyright holders.

The need for tangible storage media

Neither French nor European law allow for the rule of exhaustion to apply to digitally-stored works. The European Court of Justice, when discussing the notion of "products" in the Deutsche Grammophon case, referred to any tangible good dedicated to the storage of a sole copyrighted work, as those goods can be sold to customers. This stands in contrast to a digital storage method that would allow multiple copies to be made instantaneously as part of a service provision.

This has been further implemented in European law, under Article 4 of the Directive on the harmonisation of certain aspects of copyright and related rights in the information society,[ii] pursuant to which the right of exhaustion only applies where tangible copies are concerned.[iii] French law seems to comply with these EU provisions as the rule of exhaustion is restricted to tangible copies under Article L. 122-3-1 of the French intellectual property code.

In a digitalized world which knows no barriers and where copies of an original work are no longer fixed to dedicated physical media and may be reproduced infinitely, it is generally considered that the rule of exhaustion does not apply. Contrary to this, however, the rule has been extended to copyrighted software.

Exhaustion of rights with software

In France, Article L 122-6, 3° of the French Intellectual Property code does not expressly use the term "tangible copies" to designate that copies of software are

i ECJ, 8 June 1971, Deutsche Grammophon GmbH v Metro-SB-Großmärkte GmbH & Co. KG.: C-78/70
ii Directive #2001/29/EC of 22 May 2001: OJ *L 167 , 22/06/2001 P. 0010 - 0019*
iii Recital 29 of the Directive

subject to the rule of exhaustion, but instead uses the term "versions". This change in vocabulary could imply an application of the rule to intangible copies. Nevertheless, French courts have not explicitly ruled on this issue.

The European Court of Justice first acknowledged the application of the rule of exhaustion to intangible media in *UsedSoft v Oracle.*[iv] In the case, a licence agreement had been assigned by the original licensee to a third party without the licensor's consent. Said third party had then downloaded the latest version of the licensed computer program provided by the licensor on its own website, and had installed it on its computer.

The licensor sued the third party on the grounds of copyright infringement, claiming that it had not authorized the licence assignment, due to the fact that the rights were not exhausted in the absence of the sale of a physical copy of the computer program. However, the Court rejected the copyright holder's claims, stating that "*the transfer by the copyright holder to a customer of a copy of a computer program, accompanied by the conclusion between the same parties of a user licence agreement, constitutes a 'first sale … of a copy of a program'*" which, in the absence of distinction between tangible and intangible copies under the Directive on the protection of computer programs,[v] leads to the exhaustion of copyright.

However, legal doctrine considers this particular copyright exhaustion to only apply to computer programs. Where complex works incorporating a computer program and other copyrighted material are concerned, it is generally admitted that copyright exhaustion applies only to tangible copies[vi].

It remains that copyright exhaustion is limited in the digital world, leading operators to rely on alternative legal techniques to spread copyrighted works throughout the single market.

Bypassing the lack of copyright exhaustion

Although copyright exhaustion scarcely applies on digitally-stored copyrighted works, both case and statutory law offer solutions for the use of copyrighted material on the Internet.

Communicating a copyrighted work to the same public via several websites

Under Article 3 of Directive no. 2001/29/CE, copyright holders have the exclusive right to communicate their works to the public. Nevertheless, EU case law[vii] indicates that this provision only applies to the first communication either:

- via a determined type of media (e.g. public websites, CD, DVD, book, etc.); or
- to a determined public which would not have been reached otherwise.

In other words, once the work has been communicated for the first time on a public website, an individual may use it on his own website without needing to pay an additional royalty to the copyright holder.

This rule was clearly stated in a case which involved two people broadcasting a video stored on YouTube, but copyrighted by a competitor, on their own website. The competitor raised a plea for copyright infringement. However, the ECJ ruled that framing a copyrighted work should not be deemed as a new communication under Article 3 of Directive no. 2001/29/EC, as it was not targeted towards a public different to that which it had already been communicated to. Due to the fact that the first communication took place on a free website, the public was considered to be all the users of the Internet.[viii] The solution would be different in cases where the copyrighted material had been published without the copyright holders' consent[ix] or on a limited-access website (limited by means of a login and password).

Although current case law allows for a wide use of copyrighted material, it prevents copyright holders from controlling the broadcast of their works. That is why EU statutory law is currently implementing a new global licence system for the broadcast of copyrighted material.

Adapting copyright law to new Internet practices

Due to the difficulty in managing copyright on the Internet, EU legislation is now aiming at implementing cross-border licences, in order for copyright holders to broadcast their material to a wider pool of users.

To that end, a new Directive[x] aims at allowing collective management organizations to conclude cross-border licences with streaming companies, in order to give them access to a wider repertoire in consideration for remuneration to copyright holders.

For the moment, this Directive has not been implemented into French legislation. However, it will likely allow for the wider development of streaming in Europe. Although this may appear as a type of setback compared to the rule of exhaustion, it gives access to a larger scope of material, which will benefit EU consumers.

iv ECJ, 3 July 2012, UsedSoft GmbH v Oracle International Corp.: C-128/11
v Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (OJ 2009 L 111, p. 16)
vi ECJ, 31 January 2014, Nintendo v PC Box: C-355/12
vii ECJ, 7 December 2006, SGAE v Rafael Hoteles SA: C-306/05
viii ECJ, 21 October 2014, BestWater International GmbH v Michael Mebes & Stefan Potsch: C-348/13
ix French Cour de cassation, 1st civil Chamber, 12 July 2012: Bull. Civ. I, no. 166
x Directive #2014/26/EU of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market: OJ L 20 March 2014, L 84/72

Barcelona/Madrid: Proposal for a Directive on contracts for the online and other distance sales of goods: another step towards the Digital Single Market

On 9 December 2015, the European Parliament and the Council approved a proposal for a Directive covering certain aspects of contracts for the online and other distance sales of goods.

This Proposal is another initiative taken by the European Union in order to develop the European Digital Single Market strategy ("**DSM**"), which has been identified by the European Commission as one of its 10 political priorities. The DSM aims to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy.

A grain of sand

The Proposal can only be understood in the broader context of the DSM. This strategy, which was approved by the European Commission in 2015, is directed to remove existing online barriers within the European Union.

The DSM lies on three main pillars: the **first pillar** aims to grant better access for consumers and businesses to digital goods and services across Europe; the **second pillar** consists in creating the right conditions and a level playing field for digital networks and innovative services to flourish; and the **third pillar** will be focused on maximising the growth potential of the digital economy.

In words of President Mr Jean-Claude Juncker, "*you can drive from Tallinn to Turin without once showing your passport. But you can't stream your favourite TV shows from home once you get there*". This is what DSM is about.

In this context, the Proposal is just one of the specific actions to be undertaken under the umbrella of the DSM. In particular, the Proposal falls within the scope of the first pillar of the strategy, the removal of online barriers in the European Union.

Key Issues

- The Proposal has been approved in the context of the DSM.
- The Proposal will apply to online and other distance sales of goods conducted between business and consumers.
- The Proposal provides consumers with a higher level of protection.

The Proposal in a nutshell

The Proposal aims to harmonize certain aspects of each Member State's legislation on the online and other distance sales of goods concluded between business and consumers.

The intention behind this Proposal is for both businesses and consumers to gain confidence in selling and purchasing online and across borders.

According to the Proposal, it will apply (i) to sales of goods contracts, (ii) online, and (iii) between business and consumer. Conversely, it will apply neither to distance contracts for the provision of services nor to any durable medium incorporating digital content where the durable medium has been used exclusively as a carrier for the supply of the digital content to the consumer (e.g., DVD).

Summary of key changes

The main changes that the Proposal will enact in Member States' national mandatory rules that apply to consumer sales contracts will be the following:

(i) Hierarchy of remedies: if a good is non-conforming, a consumer will be first required to request repair or replacement. Only as a second step can the consumer ask for termination of the contract or a price reduction.

(ii) Duty to notify by the consumer: Member States will be no longer authorised to stipulate that in order to benefit from their rights, consumers must inform the seller of the defect within a certain period of time from its discovery (most Member States set out this timeframe in two months). Thus, the duty to notify will be removed.

(iii) Reversal of the burden of proof: a consumer can only ask for a remedy if the good was non-conforming when delivered. The burden of proof will be reversed during the first two years, and the business will be obliged during this period to provide that no such defect existed at the time of delivery of the product.

As it can be seen from these provisions, the Proposal grants consumers a higher level of protection.

What next?

The Proposal was approved on 9 December 2015. According to the European legislative process, the Proposal needs to be approved both by the European Parliament and by the Council, which may take approximately one year.

According to the current text of the Proposal, once the Proposal has been approved as a Directive, Member States will have two years to implement the Directive in their national legal systems.

Therefore, the effects the Proposal may provoke on business and consumers are foreseen on a mid-term basis.

Congratulations to our Spanish Team!

As for the fourth time, our Barcelona IP Team has been awarded with the IP Firm of the Year Award 2016 from the prestigious sector publication Managing Intellectual Property, award that our team has already won on three previous occasions (2008, 2012, 2014 and now 2016).

Chambers and Partners 2016, Life Sciences: Patent Litigation: Spain – **Band 1**

Best of The Best 2016 – Top 30 Patent practitioners in the World

Miquel Montañá has been identified among the **Top 30 Patent practitioners in the World** and will be included in the **Best of The Best Expert Guide**, list of the global elite which is published only every two years by Euromoney Legal Media Group.

Barcelona/Madrid: Geo-blocking practices and other forms of discrimination in online sales in the spotlight of the European Commission

The e-commerce sector inquiry conducted by the European Commission (the "**Commission**") shows that geo-blocking in online sales may raise antitrust concerns under Article 101 of the Treaty on the Functioning of the European Union ("**TFEU**"), which prohibits agreements that may disrupt free competition within the internal market. The Commission has recently published a Proposal for a Regulation addressing geo-blocking and other forms of discrimination.

The prevention of unjustified geo-blocking practices constitutes one of the actions to be implemented within the Digital Single Market Strategy adopted by the Commission, according to which one of the main pillars is to ensure better access for consumers and businesses to consumer and digital goods and services across the European Union ("**EU**").

On 18 March 2016, the Commission published its Staff Working Document on "*Geo-blocking practices in e-commerce. Issues paper presenting initial findings of the e-commerce sector inquiry conducted by the Directorate-General for Competition*" (SWD (2016) 70 final) ("**Geo-blocking SWD**"). On 25 May 2016, the Commission published a Proposal for a Regulation on geo-blocking and other forms of discrimination (COM (2016) 289 final) (the "**Proposal**").

What is geo-blocking?

Geo-blocking is defined as any commercial practice conducted by online providers which prevents consumers from accessing and purchasing consumer goods or digital content services offered, based on the location of the consumer in a Member State being different to that of the provider (see §32 of the Geo-Blocking SWD). Examples of geo-blocking are: (i) blocking access to websites for consumers located in other Member States, (ii) automatic re-direction of consumers to another website of the same or a different service provider (for example one that is located in the same Member State as the consumer), and (iii) refusing delivery and/or payment when the consumer is located in a different Member State from that of the provider (see §35 of the Geo-Blocking SWD).

Key Issues

- Geo-blocking may raise antitrust concerns when retailers or service providers are contractually obliged to geo-block.
- The Proposal for a Regulation published by the Commission seeks to prevent geo-blocking and other forms of discrimination.

Geo-blocking should be distinguished from geo-filtering. Geo-filtering refers to those commercial practices pursuant to which online providers allow consumers to access and purchase their consumer goods or digital content services cross-border, but with different terms and/or conditions depending on the location of the consumer. For example, a consumer in a different Member State to that of the online provider may be charged at a higher price than a consumer located in the same Member State as the online provider (see §33 of the Geo-Blocking SWD).

The Geo-blocking SWD main findings

The Geo-Blocking SWD gathers together the results of the competition sector inquiry launched by the Commission in order to analyse whether competition could be restricted or distorted in the e-commerce sector.

Through this inquiry the Commission verified that, although in some cases the geo-blocking practices applied to consumers would be based on unilateral decisions adopted by the retailer or the service provider not to sell cross-border, there were cases in which they recognised facing contractual restrictions on their ability to sell cross-border, which lead to geo-blocking practices.

The Commission states that when geo-blocking is adopted unilaterally by non-dominant companies it falls outside the scope of the EU antitrust rules, as Article 101 of the TFEU expressly requires the existence of an "*agreement*" or a "*concerted practice*" between undertakings. However, when retailers are contractually obliged by their providers to geo-block, this practice may raise antitrust concerns under the EU antitrust regulations.

Proposal for a Regulation on geo-blocking and other forms of discrimination

The Proposal seeks to prevent discrimination in online sales based on the nationality, place of residence or place of establishment of the consumer, on the basis of the non-discriminatory principle set out in Article 20(2) of Directive 2006/123/EC.

The main provisions of the Proposal are:

a) It prohibits the blocking of access to online interfaces on the basis of customers' residence and the rerouting of customers, unless they have given their express consent (Article 3).

b) In relation to access to the goods or services, it prohibits discrimination against customers in the following situations: (i) where the trader is not involved in the delivery of the product or service to the customer's Member State, (ii) where the trader provides electronically supplied services, other than services whose main feature is the provision of access to and use of copyright protected works or other protected subject matter, and (iii) where the services are provided by the trader in a Member State different from that of the customer's Member State of residence (Article 4).

c) It lays down non-discrimination rules specifically in the context of payments (Article 5).

d) It establishes that agreements with traders containing passive sales restrictions which would lead to violations of the rules set out in the Proposal are automatically void (Article 6).

This Proposal has been notified to the EU Parliament and the Council and will follow the corresponding EU legislative process for its approval.

Frankfurt: "Implementation Day": Green light for business deals after easing of Iran Sanctions?

On 16 January 2016, the Implementation Day under the Joint Comprehensive Plan of Action ("**JCPOA**") took place. The International Atomic Energy Agency confirmed that Iran complied with the first of its crucial obligations of scaling back its operations as stated in the nuclear agreement. In return, the international sanctions have been partly lifted and areas for business opportunities have re-opened. However, despite some headlines implying otherwise, one needs to be mindful that there are still many restrictions in place with respect to business with Iran. Therefore, any intended deal must undergo strict scrutiny, in particular, when it comes to the transfer of technology. It must also be noted that the treatment of sanctions vastly differs between the EU and US.

EU Sanctions

The lifting of EU sanctions against Iran (as stipulated in Council Regulations [EU] 2015/1861 and 2015/1862) concerns, in particular, the facilitation of financial and trade activities. Moreover, it also involves many Iranian individuals and entities being taken off sanctions lists. This means that entering into business relationships with such individuals and entities is now possible.

With respect to the financial sector, authorization and notification requirements for money transfers to and from any Iranian individuals and entities have been lifted. Furthermore, Iranian banks are now once again free to establish subsidiaries in the EU and can be connected to special messaging systems like SWIFT. These entitlements are, however, subject to the condition that the Iranian business partner is not included in any of the remaining sanctions lists. Moreover, certain Iranian banks, such as Bank Saderat Iran, Bank Saderat plc, or Bank Refah will still remain on sanctions lists. These sanctions lists will also still apply to a significant number of Iranian persons and entities due to their links with nuclear proliferation activities.

Key Issues

- After Implementation Day on 16 January 2016, a significant number of international nuclear-related sanctions against Iran have been lifted whereas others still remain in force
- There has been an extensive easing of EU sanctions against Iran
- The US has only limited which sanctions have been lifted, mainly US secondary sanctions concerning non-US persons. US primary sanctions remain in place
- The "snap-back" mechanism allows for EU and US sanctions to be re-imposed in the event that Iran violates its obligations under the Nuclear Deal
- Embargoes on Iran relating to human rights violations and terrorism remain in place

Further relaxations of EU sanctions relate to the provision of insurance and re-insurance, the import and export of gold, precious metals and the transport sector. EU sanctions affecting the energy sector haven also been lifted, in particular, with respect to oil, gas and petrochemicals. For instance, importing such goods, exporting technological equipment, and providing technical assistance in this industry are no longer sanctioned.

However, it is important to note that certain EU sanctions against Iran, in particular, the embargos resulting from human rights violations and terrorism have been unaffected by Implementation Day.

Against this background, from an EU sanctions perspective many business areas, in particular, business deals with "Enterprise Resource Software" are, in principle, not penalized anymore, provided that the goods are not specifically designed for use in nuclear or military facilities.

US Sanctions

The United States have, in comparison, been more restrictive regarding the lifting of sanctions against Iran. The easing of US sanctions primarily concerns "US secondary sanctions", which are prohibitions of transactions by Iran-related, foreign individuals acting

outside of US jurisdiction. Violations of this type were an especially notable risk for foreigners as they may have ended up on a US sanctions list. As a consequence of easing US secondary sanctions, non-US individuals are free to enter into transactions in the automobile, shipping, shipbuilding, port building as well as the energy sector. Even trading with gold and other precious metals is legal again.

Furthermore, trade sanctions concerning graphite, raw or semi-finished metals such as aluminum, steel, coal, and software for integrating industrial processes, in connection with activities that are consistent with the JCPOA, have also been lifted.
The financial sector and the provision of insurance and re-insurance have also been subject to liberalizations. In principle, the lifting of sanctions also encompasses the provision of associated services in those sectors.

Nevertheless, all transactions concerning any specific US element, thus covered by "US primary sanctions", still remain in place and bear significant compliance risks for affected individuals and entities. Against this background, an Iran-related deal would be subject to US primary sanctions if it involved, for example, US persons (including US citizens or US green-card holders), US incorporated entities (including foreign branches), the US territory or the US financial system (in particular when using US dollars as transaction currency). The same applies to the transfer of goods originating from the US as well as foreign goods containing more than a *de minimis* percentage of US origin (generally more than 10%). Whenever one of the aforementioned US elements applies, Iran-related transactions are prohibited under US primary sanctions.

All transactions with individuals and entities still covered by the vast US sanctions lists, in particular the list of Specially Designated Nationals (SDNs) imposed by the US Treasury's Office of Foreign Assets Control ("**OFAC**"), also remain prohibited.

In this regard, OFAC has only licensed certain transactions involving non-US subsidiaries owned or controlled by US persons without any participation of the US parent companies, such as the import of Iranian carpets as well as foodstuffs. In addition, it is possible to acquire a base-to-base licence from OFAC with respect to the export of aircrafts and related parts and services.

Snap-Back

When entering the Iranian market, clients should keep in mind that the EU and the US are free to re-impose the sanctions if Iran violates its obligations arising from the nuclear agreement. This so called "snap-back" is stipulated in the JCPOA. In case of such a snap-back, the sanctions will not come into force retroactively. Nevertheless, contract designs should also include rules for the resurrection of sanctions if entities decide to re-enter into Iran-business.

Further Restrictions

As mentioned above, besides the nuclear related EU and US sanctions against Iran, the embargos as a result of human rights violations and terrorism remain unaffected after Implementation Day. In addition, there are also other foreign trade restrictions and authorization requirements to be kept in mind. Of particular importance are the provisions of the EC Dual-Use-Regulation (Council Regulation [EC] 428/2009). Among other things, it governs the export of technology and software, both in physical and digital manner, which can be utilized for military as well as civil purposes respectively and thus also regulates the mere transfer of knowledge. Any such export to Iran would be subject to prior authorization from the competent EU authority (for example the Federal Office for Economic Affairs and Export Controls in Germany).

Conclusion

Generally, lifting the international sanctions against Iran has opened new business areas, particularly in the technology sector. However, before entering into specific transaction in Iran, certain compliance procedures will need to be undertaken and companies should carefully evaluate whether the remaining restrictions regarding business in Iran apply to the transaction in question. Special attention should be given to the US elements since, in particular, US primary sanctions remain in place and bear significant risks for acting individuals and entities. The EU and the US have separately published guidelines with frequently asked questions relating to practical issues in connection with the lifting of international sanctions against Iran. These can be used to assist in the first instance. However, in case of any doubt, external legal advice should be obtained in advance in order to avoid severe criminal and administrative law penalties for those involved.

Brief description:

A number of international Sanctions against the Iran were lifted on January 16, 2016. New business opportunities re-opened, but with them new compliance challenges.

Links:

1. Information Note on EU sanctions to be lifted under the JCPOA: http://eeas.europa.eu/top_stories/pdf/iran_implementation/information_note_eu_sanctions_jcpoa_en.pdf

2. Frequently Asked Questions Relating to the Lifting of Certain U.S. Sanctions under the Joint Comprehensive Plan of Action (JCPOA) on Implementation Day: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/jcpoa_faqs.pdf

3. Previous briefings from Clifford Chance on this subject:

   (a) Iran Sanctions Deal – What to Expect, and When http://www.cliffordchance.com/briefings/2015/07/iran_sanctions_dealwhattoexpectandwhen.html

   (b) Iran Sanctions Deal – Managing Your Risks While Preparing for the New Landscape: http://www.cliffordchance.com/briefings/2015/08/iran_sanctions_dealmanagingyourriskswhil.html

   (c) Iran Sanctions Deal – new Adoption Day measures pave the way for sanctions relief: http://www.cliffordchance.com/briefings/2015/10/iran_sanctions_dealnewadoptiondaymeasure.html

   (d) Iran Sanctions "Implementation Day": What You Need To Know: http://www.cliffordchance.com/briefings/2016/01/iran_sanctions_implementationdaywhatyo.html

Acknowledgements

We would like to thank the following people for their contributions to this publication:

Giulia Abbagnale
Rais Amils
Petra Belova
Anna Blest
Alexander Cappel
Marcin Czarnecki
Luciano Di Via
Fabio Guastadisegni
Krzysztof Hajdamowicz
Ling Ho
Nicolas Hohn-Hein
Nadia Jagusiak
Michal Jasek
James Jeffries-Chung
Matthieu Juglar
Ines Keitel
Alvin Khodabaks
Sunny Kumar
Diego de Lammerville
Emmanuelle Levy
Montserrat Lopez-Bellosta
Vanessa Marsland
Sonia Masco
Andrei Mikes
Claudia Milbradt
Miquel Montana
Josep Montefusco
Sara van Mourik
David Pasewaldt
Jochen Pörtge
Gerson Raiser
Florian Reiling
Monica Riva
Konrad Rominkiewicz
Ashwin van Rooijen
Shila Ruff
Ludvik Ruzicka
Manel Santiliari
Anja Schwarz
Sybille Sculy-Logotheti
Leigh Smith
Eugenia Tonello

Contacts

Belgium

Thomas Vinje
Partner, Brussels
T: +32 2 533 5929
E: thomas.vinje
@cliffordchance.com

China

Ling Ho
Partner, Hong Kong
T: +852 2826 3479
E: ling.ho
@cliffordchance.com

France

Diego de Lammerville
Partner, Paris
T: +31 4405 2448
E: diego.delammerville
@cliffordchance.com

Emmanuelle Levy
Senior Associate, Paris
T: +31 1 4405 2439
E: emmanuelle.levy
@cliffordchance.com

Germany

Claudia Milbradt
Partner, Düsseldorf
T: +49 211 4355 5962
E: claudia.milbradt
@cliffordchance.com

Florian Reiling
Lawyer, Düsseldorf
T: +49 211 4355 5964
E: florian.reiling
@cliffordchance.com

Italy

Fabio Guastadisegni
Partner, Milan
T: +39 02 80634 353
E: fabio.guastadisegni
@cliffordchance.com

Monica Riva
Counsel, Milan
T: +39 02 80634 383
E: monica.riva
@cliffordchance.com

Japan

Hidehiko Suzuki
Partner, Tokyo
T: +81 3 5561 6662
E: hidehiko.suzuki
@cliffordchance.com

Poland

Krzysztof Hajdamowicz
Counsel, Warsaw
T: +48 22429 9620
E: krzysztof.hajdamowicz
@cliffordchance.com

Romania

Mihaela Mindru
Counsel, Bucharest
T: +40 21 6666 137
E: mihaela.mindru
@cliffordchance.com

Russia

Torsten Syrbe
Partner, Moscow
T: +7 495725 6400
E: torsten.syrbe
@cliffordchance.com

Spain

Miquel Montañá
Partner, Barcelona
T: +34 93 344 2223
E: miquel.montana
@cliffordchance.com

Montserrat López-Bellosta
Of Counsel, Barcelona
T: +34 93 344 2255
E: montserrat.lopez-bellosta
@cliffordchance.com

The Netherlands

Alvin Khodabaks
Partner, Amsterdam
T: +31 20 711 9374
E: alvin.khodabaks
@cliffordchance.com

UK

Vanessa Marsland
Partner, London
T: +44 20 7006 4503
E: vanessa.marsland
@cliffordchance.com

US

Daryl Fairbairn
Counsel, New York
T: +1 212 878 4960
E: daryl.fairbairn
@cliffordchance.com

CLIFFORD
CHANCE

Worldwide contact information
35* offices in 25 countries

Abu Dhabi
Clifford Chance
9th Floor, Al Sila Tower
Abu Dhabi Global Market Square
PO Box 26492
Abu Dhabi
United Arab Emirates
T +971 2 613 2300
F +971 2 613 2400

Amsterdam
Clifford Chance
Droogbak 1A
1013 GE Amsterdam
PO Box 251
1000 AG Amsterdam
The Netherlands
T +31 20 7119 000
F +31 20 7119 999

Bangkok
Clifford Chance
Sindhorn Building Tower 3
21st Floor
130-132 Wireless Road
Pathumwan
Bangkok 10330
Thailand
T +66 2 401 8800
F +66 2 401 8801

Barcelona
Clifford Chance
Av. Diagonal 682
08034 Barcelona
Spain
T +34 93 344 22 00
F +34 93 344 22 22

Beijing
Clifford Chance
33/F, China World Office Building 1
No. 1 Jianguomenwai Dajie
Beijing 100004
China
T +86 10 6505 9018
F +86 10 6505 9028

Brussels
Clifford Chance
Avenue Louise 65
Box 2, 1050 Brussels
T +32 2 533 5911
F +32 2 533 5959

Bucharest
Clifford Chance Badea
Excelsior Center
28-30 Academiei Street
12th Floor, Sector 1,
Bucharest, 010016
Romania
T +40 21 66 66 100
F +40 21 66 66 111

Casablanca
Clifford Chance
169 boulevard Hassan 1er
20000 Casablanca
Morroco
T +212 520 132 080
F +212 520 132 079

Doha
Clifford Chance
Suite B
30th floor
Tornado Tower
Al Funduq Street
West Bay
P.O. Box 32110
Doha, Qatar
T +974 4 491 7040
F +974 4 491 7050

Dubai
Clifford Chance
Level 15
Burj Daman
Dubai International Financial Centre
P.O. Box 9380
Dubai, United Arab Emirates
T +971 4 503 2600
F +971 4 503 2800

Düsseldorf
Clifford Chance
Königsallee 59
40215 Düsseldorf
Germany
T +49 211 43 55-0
F +49 211 43 55-5600

Frankfurt
Clifford Chance
Mainzer Landstraße 46
60325 Frankfurt am Main
Germany
T +49 69 71 99-01
F +49 69 71 99-4000

Hong Kong
Clifford Chance
27th Floor
Jardine House
One Connaught Place
Hong Kong
T +852 2825 8888
F +852 2825 8800

Istanbul
Clifford Chance
Kanyon Ofis Binasi Kat. 10
Büyükdere Cad. No. 185
34394 Levent, Istanbul
Turkey
T +90 212 339 0000
F +90 212 339 0099

Jakarta**
Linda Widyati & Partners
DBS Bank Tower
Ciputra World One 28th Floor
Jl. Prof. Dr. Satrio Kav 3-5
Jakarta 12940
T +62 21 2988 8300
F +62 21 2988 8310

London
Clifford Chance
10 Upper Bank Street
London
E14 5JJ
United Kingdom
T +44 20 7006 1000
F +44 20 7006 5555

Luxembourg
Clifford Chance
10 boulevard G.D. Charlotte
B.P. 1147
L-1011 Luxembourg
T +352 48 50 50 1
F +352 48 13 85

Madrid
Clifford Chance
Paseo de la Castellana 110
28046 Madrid
Spain
T +34 91 590 75 00
F +34 91 590 75 75

Milan
Clifford Chance
Piazzetta M. Bossi, 3
20121 Milan
Italy
T +39 02 806 341
F +39 02 806 34200

Moscow
Clifford Chance
Ul. Gasheka 6
125047 Moscow
Russia
T +7 495 258 5050
F +7 495 258 5051

Munich
Clifford Chance
Theresienstraße 4-6
80333 Munich
Germany
T +49 89 216 32-0
F +49 89 216 32-8600

New York
Clifford Chance
31 West 52nd Street
New York
NY 10019-6131
USA
T +1 212 878 8000
F +1 212 878 8375

Paris
Clifford Chance
1 Rue d'Astorg
CS 60058
75377 Paris Cedex 08
France
T +33 1 44 05 52 52
F +33 1 44 05 52 00

Perth
Clifford Chance
Level 7
190 St Georges Terrace
Perth WA 6000
Australia
T +618 9262 5555
F +618 9262 5522

Prague
Clifford Chance
Jungamannova Plaza
Jungamannova 24
110 00 Prague 1
Czech Republic
T +420 222 555 222
F +420 222 555 000

Riyadh
Clifford Chance
Building 15, The Business Gate
King Khalid International Airport Road
Cordoba District, Riyadh, KSA.
P.O.Box: 3515, Riyadh 11481,
Kingdom of Saudi Arabia
T +966 11 481 9700
F +966 11 481 9701

Rome
Clifford Chance
Via Di Villa Sacchetti, 11
00197 Rome
Italy
T +39 06 422 911
F +39 06 422 91200

São Paulo
Clifford Chance
Rua Funchal 418 15ºandar
04551-060 São Paulo-SP
Brazil
T +55 11 3019 6000
F +55 11 3019 6001

Seoul
Clifford Chance
21st Floor, Ferrum Tower
19, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
T +82 2 6353 8100
F +82 2 6353 8101

Shanghai
Clifford Chance
40th Floor, Bund Centre
222 Yan An East Road
Shanghai 200002
China
T +86 21 2320 7288
F +86 21 2320 7256

Singapore
Clifford Chance
Marina Bay Financial Centre
25th Floor, Tower 3
12 Marina Boulevard
Singapore 018982
T +65 6410 2200
F +65 6410 2288

Sydney
Clifford Chance
Level 16, No. 1 O'Connell Street
Sydney NSW 2000
Australia
T +612 8922 8000
F +612 8922 8088

Tokyo
Clifford Chance
Akasaka Tameike Tower
7th Floor
2-17-7, Akasaka
Minato-ku
Tokyo 107-0052
Japan
T +81 3 5561 6600
F +81 3 5561 6699

Warsaw
Clifford Chance
Norway House
ul.Lwowska 19
00-660 Warsaw
Poland
T +48 22 627 11 77
F +48 22 627 14 66

Washington, D.C.
Clifford Chance
2001 K Street NW
Washington, DC 20006 – 1001
USA
T +1 202 912 5000
F +1 202 912 6000

*Clifford Chance's offices include a second office in London at 4 Coleman Street, London EC2R 5JJ. **Linda Widyati and Partners in association with Clifford Chance.
Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

www.cliffordchance.com

J201605310049158