

Client Alert

Latham & Watkins
Litigation Department

Beyond Counterfeiting: The Expanding Battle Against Online Piracy

Recent Developments in the European Union, France, Germany, the United Kingdom and the United States

With an annual financial impact in the tens of billions of dollars, online piracy has become a significant cause for concern within the music and film industries. While a worldwide consensus has been reached on the need to protect copyright and neighboring rights (together, Copyright) on the Internet, the means for enforcing these protections diverge across countries. Policing online piracy necessarily pits the individual privacy rights of users against the entitlement of the holders of Copyright (Rights Holders) to protect their assets. Countries have approached this balance differently; to date most have taken a pro-user stance, while others, such as France, have come out more aggressively in support of the Rights Holders. We discuss some of these various perspectives here as manifested in recent developments in the anti-online piracy regimes in the EU, France, Germany, the UK and the US.

France at the Forefront Against Online Piracy: From EU and French Case Law to the Hadopi Law

On 13 May 2009, after a chaotic legislative process which made international headlines, the French

Parliament finally and definitively adopted the text of the new anti-piracy law "*promoting the dissemination and the protection of the creation on the Internet*" (dubbed the HADOPI Law) which implemented a "three strikes" graduated response.¹

While the approach adopted by the EU and its member states thus far has been to attack online counterfeiting, with the HADOPI Law, France has introduced a new approach in the fight against online piracy by focusing on its source, *i.e.* the Internet users who will now legally be responsible for any use of their computer that illegally harms Rights Holders.

It should be noted that major obstacles still lie ahead for the HADOPI Law as we can expect (i) its most controversial provisions to be challenged by its opponents in Parliament before the French Constitutional Council and (ii) that it will be perceived as being contrary to the EU "Telecom Package" (which is being currently debated) given that the EU Parliament recently adopted an amendment to this Package, so-called "Amendment n°46" (previously n°138²), which directly aims to dismantle controversial provisions, such as those included in the HADOPI Law, by rendering them contrary to EU law.

"This article compares the particular approaches adopted by the European Union, France, Germany, the United Kingdom and the United States to combat online piracy."

Therefore, we may have possible occasion to revisit this new piece of legislation in the near future.

This section seeks to present what have been, until recently, the main issues raised by online piracy and the responses adopted by the EU and France. We will then consider the new HADOPI Law and its protections for Rights Holders.

At the Crossroads of Intellectual Property and Personal Data Protection: EU and French Case Law

The chief roadblock in battling online piracy has been the difficulty in identifying those individuals sharing protected files without authorization. Identifying the infringing Internet user requires both the *Internet Protocol* address (IP Address) of the computer being used, along with the information retained by Internet Service Providers (ISPs) demonstrating the user's activity of uploading or downloading protected works.

However, as mentioned previously, there has been a tension pitting intellectual property rights protection on the one side and protections of fundamental rights such as personal data and privacy on the other.

EU Case Law: Member States Free to Require ISPs to Provide Identifying Information Before Criminal and Civil Courts

The *Promusicae* Case: In this 2008 case, a Madrid Court referred questions to the European Court of Justice (ECJ)³ regarding the balance between intellectual property rights (Copyright in particular) and fundamental rights such as privacy and data protection rights. Promusicae, a non-profit organization, contested the refusal by a Spanish ISP, Telefónica, to disclose the personal information of some of its users so that it could identify the individuals engaging in illegal file-sharing via Kazaa, a *peer to peer* software.

In reaching its decision, the ECJ considered four EU Directives⁴ applicable to Information Society, data

protection or e-commerce, as well as the relevant provisions of the EU's Charter of Fundamental Rights. The ECJ found that the Directives did not obligate Member States to mandate the communication of personal data in support of Copyright protections in civil proceedings. With this decision, the ECJ sidestepped the opportunity to provide guidance to Member States. It simply reiterated the need for a fair balance between the fundamental rights of privacy and protections for intellectual property rights. The issue was returned to the national courts and legislations which must ensure that implementation of the relevant EU Directives and provisions allows this fair balance between the rights at stake.

The *Tele-2 Telecommunication GmbH Case*5: Faced with a nearly identical fact pattern, although this time in a German context, the ECJ stated recently in early 2009 that no EU Directive (in particular Directive 2004/48 read in parallel with Directive 2002/58), precludes a Member State from requiring a third-party entity to communicate personal data and Internet activity in support of the prosecution of Copyright infringement before civil courts. However, the ECJ again declined the opportunity to present guidance as to how Member States should balance intellectual property rights against fundamental rights.

European Council may Provide Guidance that ECJ has Declined to Give

While the ECJ has passed up the opportunity to make a firm statement on how the divergent rights of those involved in online piracy should be balanced, the European Council has recently stepped into the battle and may be expected to provide this missing guidance. The Council has called for action on online content and combating piracy and has recommended measures which both the Commission and member states should take to prevent piracy. In particular, the Council encourages more information being made available to consumers to make them aware of the consequences of piracy.⁶

The Commission intends to investigate cooperation procedure, or codes of conduct, between ISPs, rights-holders and consumers to ensure not only the widespread availability of online content, but also adequate protection of copyrighted work, and close cooperation on the fight against piracy and unauthorized file-sharing.

French Case Law: Rights Holders Representatives can Manually Collect IP Addresses over Internet, Without Prior Authorization from French Data Protection Authority

French civil and criminal courts have frequently ordered ISPs to disclose information identifying suspected infringing users. Nevertheless, Rights Holders are unable to enlist the courts' aid to obtain evidence from users, but must rely on prosecutors or sworn agents of collection agencies to request such evidence.⁷

This process was recently examined by the French *Cour de cassation* (the High Court of Justice or French HCJ) in a decision dated 13 January 2009.⁸ In this case, acting in accordance with Article 9 of the French Data Protection Law,⁹ the agents of two collection agencies (SACEM and SDRM) acting on behalf of certain Rights Holders, used a *peer to peer* software and a pseudonym to obtain identifying data (such as the user's IP address and ISP). The collection agencies then demanded the French courts to order the ISP to communicate the name and the identifying information corresponding to the IP address collected.

However, the validity of the manner in which the agents obtained the IP address was called into question, with the defendant arguing that this was tantamount to automated processing of personal data¹⁰ and should have been authorized first by the CNIL pursuant to the French Data Protection Law. Nevertheless, the French HCJ sided with the lower court, finding that agents of collection agencies could obtain IP addresses without prior authorization from the CNIL because "*the IP address does not make it possible to identify the person or persons [...] since only the*

legitimate authority for enquiries may obtain the user access ID" from the ISPs. In other words, this ruling states that an IP address is merely a component of identity which is not *per se* personal.

Many scholars and lawyers have understood the position taken by the French HCJ as granting the ability to obtain IP addresses over the Internet to the Rights Holders themselves. Yet a word of caution is advised here as the ruling clearly stated that the processes performed by the collection agencies' sworn agents were performed *manually* and on a case-by-case basis, therefore falling outside the scope of the CNIL. Moreover, pursuant to Article L. 331-2 of the French Intellectual Property Code (IPC), only sworn agents of collection agencies or certain professional organizations (e.g., the Agency for the Protection of Programs or Association against Audiovisual Piracy) are authorized to process personal data to uncover, document and fight online piracy.

Engaging the User Directly in Fight Against Online Piracy: The Hadopi Law

As mentioned previously, the French Parliament has only very recently settled the final text of the HADOPI Law against online piracy and for the protection of Copyright on Internet networks.¹¹ We reiterate that the HADOPI Law will likely face a challenge before the French Constitutional Council. Such constitutionality review by the Council should take a month. Then, among other administrative formalities, implementing decrees will need to be issued. One can reasonably assume that the HADOPI will start its "three strikes approach" only after the summer, at the earliest.

The Law is not France's first legislative attempt to strengthen Copyright protections. It initially did so with its Copyright Information Society Law¹² of 1 August 2006 (the DADVSI Law) which aimed to prevent the exchange of copyrighted works over *peer to peer* networks. The DADVSI Law also criminalized the violation of digital rights management (DRM)

protection measures and established an independent administrative authority, the Regulatory Authority for Technical Measures (ARMT), to regulate DRMs and the interoperability between protection software and the devices in which they are installed. The DADVSI Law came under fire as being highly technical and for presenting a direct threat to freely available software. Following a very short existence, the DADVSI Law quickly became obsolete when many of the music industry heavyweights withdrew their DRMs.

The charge against the major online file-sharers was then taken up by French ISPs and representatives of the music and movie industries in 2007. Discussions between the groups resulted in an agreement in which the ISPs agreed to monitor their users—if and once the law was modified to allow for such monitoring—so that the most active file-sharers could be identified and issued formal warnings (although the ISPs would not agree to suspend or terminate Internet services).¹³ In return for their efforts, the movie industry agreed to release movies on DVD six months following their cinema run, while the music industry would make DRM-free songs available for download.

It was this agreement between the ISPs and music and movie industries that inspired the HADOPI Law, and has made France a pioneer in legislating on the issue of online piracy. In addition to civil and criminal counterfeiting provisions, the Law establishes a new approach in the battle against online piracy by holding the user of an Internet access point directly responsible for any improper use.

Mandates and Scope of HADOPI Law

The law underlying the HADOPI Law derives from the new Article L.336-3 of the French IPC¹⁴ which creates a duty for the user of an Internet access (the User) to prevent its access from being used as a means to share (via download, upload, stream or otherwise making available to others) contents protected by Copyright without the authorization of the Rights Holders. Failure to comply with Article L.336-3 exposes the User to

sanctions pursuant to the “three strikes” procedure. Sanctions may be avoided, however, upon showing that: (i) the User has implemented one of the “technical protection means” introduced by the Law (see further description later in this article); (ii) the infringements identified were realized by an independent third party who has fraudulently used its Internet access; or (iii) that the User was unable to prevent infringement due to a *force majeure* event.

To carry out the mandates of the new Law, a new independent administrative authority with legal personality, the HADOPI, has been created to replace the ineffective ARMT. This new body will receive complaints from certain authorized representatives of the music and film industries (see later in this article), and with the cooperation of ISPs, will track down offenders. The weapon of choice for the HADOPI will be the graduated response, or three-strikes procedure, against online pirates. This new authority embodies all of the necessary rights to obtain from ISPs without any prior judicial procedure, any and all identification information and personal data of the Users identified as infringers. Apart from this primary mission, the HADOPI protects copyrighted content over the Internet, promotes the development of legal downloads of such content and oversees DRMs and identification measures.

Access to the HADOPI is limited to professional organizations (such as those mentioned previously in the context of the French Data Protection Law), royalties collecting agencies and the National Center for Cinema. Significantly, Rights Holders have not been conferred with the right to invoke the HADOPI's authority directly; the usual recourse available to Rights Holders to fight counterfeiting remains the criminal courts. Although the procedures through the HADOPI or criminal courts share the same goal of combating online piracy, actions in the criminal courts seek to penalize infringement of intellectual property, whereas the HADOPI will prosecute Users for using their computers to share protected contents. However, we

expect that as the HADOPI's authority is increasingly invoked, there will be a need for clarification between the two procedures going forward.

The HADOPI may prosecute any and all infringements occurring within the preceding six months. The procedure under which claims raised with the HADOPI are to be examined and assessed will be set out in a decree which is expected to be issued within the coming months.¹⁵ It should be noted, however, that the protections of the HADOPI will not extend to a creation or a protected content of the Rights Holders which are established and benefiting from the favorable provisions of a "tax haven". The effects of this will be rather limited because it will apply only where all of the Rights Holders of specific intellectual property are established within and benefit from such a tax haven. The agents of the professional organizations or royalties collecting agencies will have the burden of proving that at least one of the Rights Holders lives outside of a tax haven.

Sanctions Procedure: "Three strikes" Graduated Response

The three-strikes, graduated response procedure (the Sanctions Procedure) to identify illegal sharing of content on Internet networks, requires the cooperation of ISPs at each step of the process.

The Notification Stage: Suspected infringers identified by the HADOPI will first receive an e-mail warning them that illegal use of their Internet access has been detected. If similar illegal activity is perceived within six months of this initial notification, a second notification will be sent by certified mail.

The notifications, sent by the ISPs in the name of the HADOPI, will clearly specify to the Users: (i) the dates and times of the identified infringements;¹⁶ (ii) the legal consequences should the infringements continue; (iii) the legal implications for sharing protected content; (iv) the existing "technical protection means" available to prevent fraudulent use of the Internet access; (v) the damages caused to intellectual

property by unauthorized infringement of Copyright; and (vi) the contact details for communicating with the HADOPI (e.g. telephone number, e-mail and postal address).

The Optional Transactional Stage:

Should the infringements persist, the HADOPI will have the option to order: (i) the User to comply with its obligations pursuant to the new Article L.336-3 of the French IPC before a certain deadline (by implementing, for example, a labeled technical protection mean); or (ii) the suspension of Internet access for a one to three month period. The User will be required to also undertake compliance with all applicable legal obligations regarding online anti-piracy law.

The Sanction Stage: Should the User fail to comply with its obligations pursuant to Article L.336-3 of the French IPC in the year following notice of infringement, the HADOPI may (pursuant to a procedure to be set out in a forthcoming decree) order sanctions against it. The sanctions will take the form of: (i) an order suspending Internet access for a two to 12 month period; or (ii) an order that the User take all necessary measures to comply with its obligations under Article L.336-3 of the French IPC by a set deadline (by implementing, for example, a labeled technical protection mean). Upon issuing the sanctions, the User will be informed of its right to recourse (to be taken within 30 days) before a competent jurisdiction (to be named in the forthcoming decree).

The User will be responsible for payment of the Internet access pending any suspension of its services. The User will also be registered in a central database prohibiting it from subscribing to any other Internet access in France over the course of the fixed period suspending it from Internet access. ISPs will be required to consult this file prior to processing any new subscription for Internet access; failure to do so will result in a fine of up to 5,000 EUR.

While this graduated response mechanism has been described as being "adversarial," the User may only challenge the actions taken by the

HADOPI once the independent authority has entered a sanction against it. Moreover, the window of time available to the User for taking recourse, 30 days, is particularly short.

Exemption by Implementation of Certified “Technical Protection Means”

Users will be exempt from liability under the HADOPI Law if they implement a protection device or software that has been certified by the HADOPI. Article L.331-32 of the French IPC requires the HADOPI to make public all of the functionalities that will be required before a particular technical protection means will be certified by the HADOPI. The forthcoming decree will set out the procedure by which the HADOPI will grant and periodically review the certified devices.

Obligations of ISPs under HADOPI Law

Under the HADOPI Law, ISPs are now required to include in their General Conditions of Use a “clear and readable” statement of User’s relevant legal obligations as per Article L.336-3 of the French IPC, as well as all potential measures available to the HADOPI in the event that those obligations are violated. The ISPs must also expressly set out the applicable civil and criminal sanctions for violation of Copyright, along with the suspected infringer’s rights of recourse. When Users initially subscribe or renew their subscription, the ISPs must inform them of: (i) the applicable legal consequences of sharing protected contents online; (ii) the technical protection means permitting Users to prevent a violation of their obligations; and (iii) the consequences of Copyright infringements with respect to the music and film industry.

The ISPs are also required to actively and promptly with the HADOPI, particularly by communicating any and all identification data on their customers upon request of the HADOPI, and suspending Internet access at least 45 days (and not later than 60 days) following receipt of a request by the HADOPI. Failure to respect these guidelines subjects ISPs to a fine of up to 5,000 EUR.

Finally, and potentially the most significant obligation imposed upon the ISPs, when suspending Internet access, no other services such as telephone and/or television services, may be impaired. The ISP must therefore determine how to suspend Internet access without affecting the remaining services (obviously technically challenging when such service is part of a triple-play offer). The results of this new HADOPI Law are highly anticipated and will be closely scrutinized by France, as well as other countries engaged in the fight against online piracy.

The significant interest that the EU has taken in HADOPI is illustrated by the recent rejection by the Council of Telecoms Ministers of the Telecom Package mentioned previously and the unexpected and overwhelming approval of Amendment n°46 (previously n°138)¹⁷ which comes out against the HADOPI Law. In relevant part, Amendment 46 affirms that an individual’s access to the Internet constitutes a fundamental right which cannot be restricted in the absence of a ruling by a judicial authority.

Thus, it remains to be determined whether France is at the forefront of a global trend.

The UK Position

The UK position is governed by the Copyright Designs and Patents Act 1998 (CDPA). It regulates copyright and design rights and provides criminal sanctions for infringement. In the UK, as elsewhere, illegal downloading and piracy is a huge problem. It cost the music industry approximately \$300 million in 2008, and is increasingly costly to the video industry.

While there has been significant discussion in documents in the newspapers and elsewhere about seeking to make Internet Service Providers (ISPs) liable, leading to a denial of service in a “big brother” type of way, the possibility of early legislation is relatively unlikely given that the current government is unpopular and nearing the end of the electoral cycle as an election is due no later than June 2010.

There already exists means for catching downloaders which leads to financially severe penalties in one way or another. The real issue which has been debated in the UK is whether the ISPs should be liable for the acts of their customers.

Under English law there are both civil and criminal penalties and they run in parallel. The difference is that the civil standard of proof is on the balance of probabilities whereas the criminal standard is beyond reasonable doubt.

Internet Service Providers

Intellectual Property Right (IPR)

Holders are keen for ISPs to act in the role of "copyright police" and have responsibility for identifying and preventing infringement by subscribers to their networks, which has been heavily resisted by ISPs in the UK. This is reflected in, among other matters, the "technical copies" defense in Section 28A of the CDPA. There are signs that IPR holders may increasingly look to ISPs to take a more active role in policing their networks and preventing infringement, particularly in relation to subscribers' use of file sharing networks.

The UK government commissioned a report into Intellectual Property, called the "Gowers Review" in 2005. It was published in December 2006, since then little has been done. It comments on the possibility of a new act of secondary infringement which would make parties that "facilitate" file sharing liable for copyright infringement. David Lammy, the relevant government minister, is also looking at IP rights from a consumer viewpoint, but this is unlikely to see legislative action in the short term. The Gowers Review's recommendation was for self-regulation by encouraging the industry to observe a Best Common Practice document for sharing data between ISPs and rights holders and to remove access from users who engage in piracy (similar to the French approach). However, there is no enacted legislation.

The Statutory Basis

Section 97A of the CDPA states that the High Court can grant an injunction against a service provider that has

"actual knowledge" of another person using their service to infringe copyright. However, proving this is difficult.

Under the CDPA, an article is an "infringing copy" if its making constituted an infringement of the copyright in the work in question, Section 27(2). Under Section 107(1) person commits a criminal offense who, without the license of the copyright owner, *inter alia*:

- a) makes for sale or hire,
- b) imports into the United Kingdom otherwise than for his or her private and domestic use,
- c) in the course of a business,
- d) offers or exposes for sale or hire,
- e) exhibits in public, or
- f) distributes

an article which is, and which he or she knows or has reason to believe is, an infringing copy of a copyright work.

A person also commits an offense under Section 107(2) if he or she has in his or her possession an article which he or she knows, or has reason to believe, will be used to make infringing copies for sale or hire. Thus peer-to-peer free services would appear to be outside the scope of the strict wording of the statute.

The offenses under Section 107(1) are triable either way. On conviction on indictment, the maximum penalty is 10 years imprisonment and/or an unlimited fine. On summary conviction, the maximum penalty is six months imprisonment and/or a £5,000 fine. A summary offense under Section 107(2) carries maximum penalty of six months imprisonment and/or a £5,000 fine. Sections 108 and 114 of the CDPA provide for the forfeiture of infringing copies or "other articles" either to the copyright owner, produced to the court or to be destroyed.

Section 24 of the CDPA provides for secondary infringement. Under this section, copyright in a work is infringed by a person who, without the license of the copyright owner makes, imports into the UK, possesses in the course of business, or sells/offers or lets for

hire, an article specifically designed or adapted for making copies of that work, knowing or having reason to believe that it is to be used to make infringing copies. In addition, under Section 24(2) a person infringes a copyright if he or she transmits the work by means of a telecommunications system, knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in the UK or elsewhere.

It follows that there are sufficient weapons already available to deal with the problem, but the problem of peer-to-peer copying is difficult to deal with because detection is difficult and enforcement is relatively costly.

Remedies for Copyright Infringement

Copyright owners and their exclusive licensees are entitled to the following remedies for infringement:

- damages may be awarded to compensate a claimant for harm caused by infringement, but will not be available where the infringement is innocent (*Sections 96 and 97, CDPA*);
- interim or final injunctions are also commonly sought in IP disputes in order to prevent an alleged infringer from continuing the infringing acts (*Section 96, CDPA*); and
- further specific remedies are also available, such as delivery up of infringing copies or articles (*Section 99, CDPA*).

These are civil remedies, and the court will award damages. The real punishment is attorney's fees, which follow the result of the litigation. While damages may only be £5,000 (\$7,500), attorney's fee may be as high as £20,000 or more (\$30,000). That can be ruinous to the average householder.

Confiscation: Proceeds of Crime Act 1995

The Criminal Justice Act 1998 (Confiscation Orders) Order 1995 extended the arrangements of the Proceeds of Crime Act 1995 to copyright offenses tried in the magistrates court.

Any prosecutor has the power to apply for a confiscation order following a conviction in the magistrates court under Section 107(1), (2) or (3) of the CDPA or any conviction in the Crown Court. The court has a duty to initiate a confiscation process when the prosecutor has given written notice that it would be appropriate to make a confiscation order or the court decides to proceed at its own volition.

Copyright and Related Rights Regulations 2003 — Enforcement

The UK implemented the Copyright Directive by the Copyright and Related Rights Regulations 2003 (*SI 2003/2498*) (Copyright Regulations), which came into force on 31 October 2003 and amends the CDPA. The only relevant substantial amendment to UK copyright law on exclusive rights was to ensure that rightholders are able to control the communication of their work to the public by means of electronic transmissions (*Section 20, CDPA*). As a result, the definition of "broadcast" has been amended so that it covers any broadcasting for simultaneous reception, whether by wireless or cable transmission (*Section 6, CDPA*). This might catch peer-to-peer downloaders.

The Copyright Regulations have now increased the protection given to effective "technological measures," which are broadly defined as any technology, devices or components designed to protect a copyright work. While the pre-existing provisions of the CDPA regarding technological measures have been substantially retained for computer programs, civil remedies against those who circumvent technological measures have been introduced for other works (*Sections 296ZA and 296ZB, CDPA*). In addition, both civil and criminal sanctions may be taken against those who make or deal in devices designed to enable the circumvention of technological measures (*Section 296ZD, CDPA*).

Online Streaming

In *UEFA & ors v Briscomb & ors* [2006] EWHC 1268, the High Court considered whether the unauthorized online streaming of live sporting events could infringe copyright. The Union of European Football Associations (UEFA) owns copyright in the live broadcasts of football matches in the European Champions League and ancillary works. The defendants operated a Web site that distributed the broadcasts over the Internet for their subscribers' viewing. The broadcasts were digitally captured and processed into signals that could be sent in "packets" over the Internet. Each part of the broadcasts was copied during processing and again on the computer of each of the subscribers who received the stream.

The court gave summary judgment for the claimants, holding that the defendants had infringed copyright in the broadcasts by:

- communicating the broadcasts or authorizing their communication to the public (*Section 20, CDPA*); and/or
- copying them (or authorizing others to make copies) (*Section 17, CDPA*).

User Generated Content Providers

The rise of user generated content (UGC) services has been huge. Sites such as YouTube encourage Internet users to upload video clips they produce onto the site, where they can be viewed and downloaded.

As demonstrated by Viacom's recent lawsuit against Google/YouTube in the US, there is now a greater focus on legal issues raised by UGC, particularly in relation to copyright. Where users own the copyright in the clips they upload, UGC providers must ensure they get a license from the user to make use of this content. The risk for UGC providers is when users include in their clips copyright works (for example, music or films) that are owned by third parties.

In the UK, providing UGC-related services is most likely to infringe the following primary rights that are exclusively available to the owner of the third party copyright:

- **The reproduction right (Section 17, CDPA).** Storing uploaded UGC on servers and making further technical copies during transmission may infringe this right.
- **The communication to the public right (Section 20, CDPA).** "Broadcasting" or "making available" the UGC may infringe this right, which can be particularly troublesome for a UGC provider. This is because the making available limb is potentially broad enough to include simply providing a link to UGC that contains infringing materials. This argument is as yet untested in the UK.

Additionally, IPR holders may bring an action against a UGC provider for "authorizing" copyright infringement, by providing its users with the means of uploading infringing content and allowing other users to stream and/or download that content. The leading UK case on this issue is *CBS Songs Ltd v Amstrad Consumer Electronics plc* [1988] AC 1013, in the House of Lords. This case, which involved twin deck tape recorders, where the second tape deck was designed for easy copying, provides that a party does not authorize infringement if:

- it does not "sanction, approve or countenance" the infringement of copyright; or
- the technology can be used for legitimate purposes.

This case might be decided differently today.

Despite these protections, in the current climate UGC providers are right to be concerned that the courts may reappraise longstanding theories of indirect copyright liability to find them liable. But the statutory remedies are available. Their real complaint relates to the difficulty of detection and the cost of related court proceedings in a society where the criminal justice system is overloaded, the authorities are reluctant to prosecute in all but the worst cases.

The German Legislative Framework Applicable to Online Piracy

In Germany, there is no similarly restrictive legislative framework as in France and there currently are no pending legislation or governmental initiatives comparable to the HADOPI Law, either. The German Federal Government, in its 2008 Media and Communication Report, advocates the development of cooperative approaches between Rights Holders and Internet Service Providers. With regard to the approach suggested by the HADOPI Law, the German Federal Government is, however, rather reluctant because it includes the transfer of personal data of Internet users, which would have to be reconciled with the secrecy of telecommunications, the right of informational self-determination and the fundamental right to the guarantee of the confidentiality and integrity of information technology systems as recently developed by the German Constitutional Court (Bundesverfassungsgericht). Thus, it seems likely that in the medium term the legal framework applicable to online piracy will continue to exist in its present form.

Main Characteristics Of Legislative and Regulatory Framework Dealing with Online Piracy

There is no legislative framework exclusively dealing with online piracy. Online piracy is mainly addressed in the Copyright Act (Urheberrechtsgesetz). Online piracy may also be affected by other laws, such as the Telemedia Act (Telemediengesetz), Telecommunication Act (Telekommunikationsgesetz), Federal Data Protection Act (Bundesdatenschutzgesetz), Civil Code (Bürgerliches Gesetzbuch) or the Criminal Code (Strafgesetzbuch).

According to the German Copyright Act, in principle, downloading or streaming content protected by Copyright without consent of the Rights Holder is illegal. The Copyright Act, however, renders legal the reproduction for private and other personal uses. According to

Section 53 (1) clause 1 of the Copyright Act, it shall be permissible to make single copies of a work for private use on any medium, provided that the copying neither directly nor indirectly serves a commercial purpose and is not made from an "original" which was obviously produced or made publicly accessible in an illegal manner. A person authorized to make such copies may also cause such copies to be made by another person, provided no payment is received therefore.

Liability of Internet Service Providers and Software Publishers

Due to difficulties in holding private Internet users liable for Copyright infringements, it has increasingly been discussed inasmuch as ISPs which services are used in the context of online piracy and software publishers whose software is used to copy and/or disseminate contents over the e-networks may be held liable for Copyright infringements.

Liability of IPSs

IPSs, as a general rule, are not responsible for information they transfer or store for its users if they do not know about the illegal acts or information and about facts and circumstances that obviously indicate such illegal acts and if they immediately remove the information or lock access thereto as soon as they learn about the infringement. Nevertheless, there is no consistent court practice on the precise scope of such provisions and the duty of care required. Some courts hold IPSs responsible for infringements of Copyright law with regard to online piracy (e.g. Regional Court Köln, dated 12 September 2007, file number 28 O 339/07). Other courts rejected liability of IPSs arguing they are neither legally nor *de facto* able to prevent such illegal actions (Higher Regional Court Frankfurt, dated 22 January 2008, file number 6 W 10/08; Regional Court Kiel, dated 23 November 2007, file number 14 O 125/07; Regional Court Düsseldorf, dated 12 December, 2007, file number 12 O 530/07).

In a recent decision, the Regional Court of Hamburg (dated 12 November 2008, file number 308 O 548/08) considered whether an Internet Access Provider is obliged to lock access to Web sites providing illegal content. The plaintiffs, five companies of the film industry, sued an Internet Access Provider for violating Copyright by providing access to a Web site on which an undeterminable person offered movies protected by Copyright for download. The court rejected the plaintiffs' application for a concerning interim injunction holding that the defendant cannot be expected to set-up DNS-blockings as they are ineffective at preventing the flow of information to users and can easily be circumvented.

Liability of Software Publishers

There is no direct liability of software publishers for Copyright infringements as they do not act themselves. However, there is indirect liability being discussed as the software publisher will usually know that its software may be used for Copyright infringement. Accordingly, with regard to peer-to-peer-software, the Higher Regional Court of Hamburg (dated 8 February 2006, file number 5 U 78/05) argued that a software provider is liable for the caused loss if the software is predominantly used for Copyright law violations and which the provider solicits as such a software. Though there is no sufficient case law in this respect it seems, nevertheless, likely that a software publisher may get around liability by informing its customers on the legal situation and the illegality of online piracy. That is to say, the Federal Court of Justice ruled in various decisions, such as its copy-shop decision, that a certain act (provision of copiers) that may be executed in a legal manner must not be prohibited but rather be accompanied by respective instructions of users.

Institutional Setup for Enforcing Copyrights

There is no specific court, government agency or other body or entity in charge of ruling upon online piracy matters, but the general civil, criminal and administrative courts are the

competent bodies according to their jurisdiction. However, according to Section 105 (1) of the Copyright Law, the state governments shall be empowered to assign by statutory order Copyright litigation to specific Local Courts. Prosecution and administrative authorities may investigate online piracy matters. Administrative authorities may also take measures to prevent Copyright violations.

Remedies for Copyright Infringements

Any Rights Holder (author or holder of the right of utilization) can sue against any person who infringes his or her Copyright. In addition, criminal sanctions may apply.

There is no exclusive right for collecting societies or professional defense organizations to bring an action. Collecting societies may only bring an action with regard to those authors who joined them and; therefore, transferred the relevant rights. In fact, most authors in Germany join a collecting society which enforces the authors' Copyright or the right of another person to use the work.

Pursuant to Section 97a of the Copyright Act, the person whose right was infringed is supposed to send the infringer a notice putting the infringer in the position to settle the dispute by issuing an omission statement which includes an adequate penalty.

Processing of Personal Data of Users Downloading, Streaming or Uploading Contents on E-Networks

There is no specific legislation but several laws apply on the issue of personal data of relevant users. According to the Federal Data Protection Act (DPA) the collection, processing and use of personal data shall be admissible only if permitted or prescribed by the DPA or any other legal provision or if the data subject has consented. As a general rule, ISPs must not transfer personal data of users (such as the IP-address) to third persons.

With regard to specific constellations, the Telecommunication Act imposes an obligation upon ISPs to provide state authorities with information regarding certain users. Thus, the competent state authorities may claim access for the purpose of, for example, prosecuting criminal and administrative offenses and danger prevention. There is no civil law right of private person (authors, other Rights Holders, collecting societies) to claim access to information disclosing the identity of a user infringing Copyright law. However, there is a right to get access to files of the state authorities in proceeding again infringers.

Due to the limitations for access to information about the identity of infringers, strong efforts have been taken by private organizations to complain about Copyright infringements to prosecution authorities, in order to get the information of the relevant user in the course of the criminal investigation. There is no consistent case law yet on the question whether a Rights Holder has a claim to access the information held by the prosecution authorities.

With regard to Copyright infringements with a commercial dimension, Section 101 of the Copyright Law grants the Rights Holder a right to information against the violator on the details of the infringement, such as the origin of the copied works and the distribution channels.

US Measures to Combat Online Piracy

Legitimate sales of digital music and videos continue to grow rapidly in the United States, but online piracy remains a vexing and costly problem for entertainment and media businesses. With the passage of the HADOPI Law in France, movie studios and record labels in France now have a powerful tool to combat online piracy, and US companies have taken note. Just days before the first vote on the measure in the French Parliament, US lawmakers were hearing calls for similar antipiracy measures. On 6 April 2009, the Foreign Affairs Committee of the House of

Representatives held a hearing near Los Angeles, California, on global copyright piracy. At the hearing, film director Steven Soderbergh referred to French plan and asked "lawmakers to deputize the American film industry to pursue copyright pirates."¹⁸

The hearing was part of a new initiative launched by Congressman Howard L. Berman, the Foreign Affairs Committee Chairman. According to a press release, the California Democrat will "soon introduce legislation that will begin to elevate the attention given to intellectual property concerns abroad."¹⁹ Details have not been released, but the aim of the initiative is to help US content-owning businesses by encouraging other countries to enforce intellectual property rights.²⁰

As director Soderbergh's comment suggests, US content-producing industries are seeking more effective measures to protect their interests. These industries have encouraged US lawmakers to reject Internet neutrality laws and have sought instead to advance laws requiring ISPs to police their networks for infringing works.²¹ So far, legislative efforts to force ISPs to act as content police have failed. Absent new legislation, companies seeking to protect their rights must either rely on existing copyright law, which may be inadequate to the task, or seek solutions beyond the law.

Direct and Indirect Infringement Claims

The governing copyright statute in the United States is the Copyright Act of 1976, as amended.²² The Copyright Act protects "original works of authorship" by giving authors exclusive rights of copying, distribution, creation of derivative works, and (where applicable) public performance and display.²³ A copyright owner may enforce its rights in a work by suing parties who directly infringe or by suing those who are secondarily liable. A copyright holder establishes a claim of direct infringement by proving that it owns a valid copyright and that the defendant actually copied the protected material.

A copyright owner may also pursue claims against third parties, generally under the theories of vicarious infringement, contributory infringement, or intentional inducement of infringement. These theories could be applied to an ISP, for example, whose users have engaged in infringing conduct. Vicarious liability requires a showing that the defendant has the right and ability to control the infringing conduct and receives a direct financial benefit from exploiting the protected works. Contributory infringement requires a showing that the defendant's conduct contributed to another's direct infringement by causing or furthering the infringement, or by providing the means to infringe. The US Supreme Court, in *Sony v. Universal Studios*,²⁴ has established a "safe harbor" from secondary liability for parties who sell equipment that enables copying but is "widely used for legitimate, unobjectionable purposes" or "capable of substantial non-infringing uses."²⁵

Under a third theory of liability, intentional inducement of infringement, a plaintiff must show that the defendant intentionally induced another party to directly infringe the protected work. This theory was developed in *MGM Studios, Inc. v. Grokster Ltd.*,²⁶ which involved a defendant who distributed free software that enabled its users to share unauthorized copies of copyrighted works online.²⁷ The US Supreme Court held that the *Sony* safe harbor did not apply because an actual purpose of the software was to cause infringement.²⁸ Establishing a new basis for contributory infringement, the court further held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."²⁹

Remedies

Remedies for infringement under US copyright law include temporary and final injunctions,³⁰ as well as the impounding and disposition of infringing articles.³¹ A copyright owner may seek

actual damages plus the defendant's profits that are attributable to the infringement (but not profits accounted for in computing the actual damages).³² In the alternative, a plaintiff may elect statutory damages within a range of \$750 to \$30,000 per work infringed, "as the court considers just."³³ The court also has discretion to award full costs and reasonable attorney's fees.³⁴

4.2 The Digital Millennium Copyright Act

The passage of the Digital Millennium Copyright Act (DMCA) in 1998 provided new tools for combating online piracy, as well protections for ISPs from secondary infringement claims.

Anti-Circumvention Provisions

The DMCA created remedies for circumventing copy-prevention systems, such as digital rights management (DRM) systems.³⁵ Civil remedies include actual damages or statutory damages between \$200 and \$2,500 per act of circumvention, with higher penalties for repeat offenders.³⁶ Criminal penalties include a fine as high as \$500,000 or five years imprisonment, with the fine or term doubling for repeat offenders.³⁷ How effective the anti-circumvention provisions are in fighting online piracy may depend as much on the practical limitations of using them as on consumer preferences and market forces. Notably, Apple, the creator of the popular iTunes music software and store, recently began selling music without DRM protection, giving consumers the choice to play music on more devices with no restrictions on copying.³⁸

Safe Harbor and Take-Down Notices

The DMCA also created a safe harbor for ISPs, which limits their liability for users who use their systems or networks to transmit infringing materials.³⁹ For the safe harbor to apply, the ISP must meet certain requirements. The ISP, for example, must not initiate the transmission, select the material or recipients, modify the material or store copies accessible to non-recipients.⁴⁰

The safe harbor also applies to information that users store on an ISP's systems or networks.⁴¹ Again, there are requirements that the ISP must meet. If the ISP has the right and ability to control the online activity, the ISP must not receive a financial benefit directly attributable to it.⁴² The ISP also must not have actual knowledge that the material or activity is infringing and must not be aware of facts or circumstances that make the infringing activity apparent.⁴³ Once the ISP obtains such knowledge or awareness, it must act "expeditiously to remove, or disable access to, the material."⁴⁴ The provision allows copyright owners to combat online piracy by sending a "takedown" notice to the ISP when infringement is suspected.⁴⁵ The notice must include an authorized signature of the complaining party, identification of the copyrighted work and the material allegedly infringing it, and a statement that the complaining party has a good faith belief that the use of the allegedly infringing material is not authorized by law.⁴⁶ While ISPs are not required to comply with takedown notices, they have an incentive to do so in order to retain their safe-harbor status and avoid potential secondary liability.

Subpoena to Identify Infringers

The DMCA also provides copyright owners with a procedure to subpoena ISPs for information relating to alleged infringers.⁴⁷ The subpoena request must include a copy of the takedown notice.⁴⁸ If issued, the subpoena authorizes and orders the ISP to "expeditiously" disclose to the complaining party "information sufficient to identify the alleged infringer [. . .] to the extent such information is available to the service provider."⁴⁹

Beyond the Law

Content-producing industries in the US may be shifting their antipiracy strategy away from the tools provided by the DMCA and other copyright laws. The strategy of initiating mass law suits against infringers has been unpopular with consumers. And while the strategy may have curbed some piracy, the

industries continue to suffer declining sales. Moreover, the industries may not be able to wait for the passage of new laws requiring ISPs to police their networks.

For several years, these industries have been quietly pushing on another front. They have been directly seeking the help of ISPs to combat online piracy. These efforts appear to be making progress. The Recording Industry Association of America (RIAA) recently announced that it had reached agreements with ISPs in which ISPs will forward a notice to customers who the RIAA suspects have engaged in infringing activity.⁵⁰ Notably, under the agreement, the RIAA would not ask for the identity of the customers, thus avoiding privacy concerns.⁵¹ Whether this approach is effective and acceptable to consumers remains to be seen.

Endnotes

- ¹ The "HADOPI Law" was named in reference to the newly established High Authority for the Dissemination of Creation and the Protection of Rights on the Internet (the "HADOPI").
- ² Please refer to endnote 17.
- ³ ECJ 29 January 2008, C-275/06, *Productores de Musica de Espana v. Telefónica de Espana (Promusicae)*.
- ⁴ Directive 2000/31 on certain legal aspects of Information Society services, in particular electronic commerce, in the internal market (Directive on electronic commerce); Directive 2001/29 on the harmonization of certain aspects of copyright and related rights in the Information Society; Directive 2004/48 on the enforcement of intellectual property rights; and Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- ⁵ ECJ 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH*, C-557/07.
- ⁶ Official Journal (2008/C 319/06), 13 December 2008.
- ⁷ See our 2007 article in which we addressed some of these issues of French case law and the position taken at that time by the French Data Protection Authority—Commission Nationale Informatique et Libertés, "CNIL": Latham & Watkins *Client Alert* no. 638 dated 22 October 2007, "At the crossroads of Intellectual Property

- and Data Protection : Latest Developments In French Case Law relating to online Piracy”.
- ⁸ Criminal chamber of the French High Court of Justice, 13 January 2009, SACEM & SDRM v. Mr. C.S., decision no. 08-84088.
- ⁹ French Data Protection Law of 6 January 1978, as amended August 2004 (relating to information technology, data filing systems and liberties).
- ¹⁰ It has been firmly established by CNIL, other European Data Protection Authorities, and the Working Party 29 created by the 95/4610 EU Directive, that IP addresses are considered personal data.
- ¹¹ In addition to the fight against online piracy, the HADOPI Law also deals with other matters linked to the regulation of the Information Society such as the calendar of media, *i.e.* the calendar for marketing cinematographic creation on different media and the conditions for the use and marketing of journalist’ creation especially on the Internet networks. We will not address those aspects of the HADOPI Law in this *Client Alert* as regards the subject and the format of this article.
- ¹² Act no. 2006-961 of 1 August 2006 on copyright and neighboring rights in the Information Society, “DADVSI Law.”
- ¹³ The agreement, signed on 23 November 2007, was termed the “Olivennes Agreement” after Denis Olivennes, the then Chair of the group’s joint report and CEO of FNAC, the largest French retailer of cultural and consumer electronics products.
- ¹⁴ French Intellectual Property Code.
- ¹⁵ New article L.331-38 of the French IPC.
- ¹⁶ The nature and the name of the content will not be specified, as this would be considered a violation of the right of privacy. The user may nevertheless obtain this information from the HADOPI.
- ¹⁷ A task force, made up of various representatives from the EU Commission, Council and Parliament, informally reached a consensus (now inexistent) in line with the HADOPI Law prior to this vote according to which the need of a prior ruling by a judicial authority was not a prerequisite (the task force was satisfied that a ruling by an independent and impartial tribunal would be rendered at some point). However, the first and current version of Amendment n°46 adopted by the EU Parliament takes an opposite stance, stating that “no restriction may be imposed on the fundamental rights and freedoms of end-users, without a prior ruling by the judicial authorities, notably in accordance with Article 11 of the Charter of Fundamental Rights of the European Union on freedom of expression and information, save when public security is threatened in which case the ruling may be subsequent.”
- ¹⁸ Kevin J. O’Brien, Plan to Curb Internet Piracy Advances in France, *The New York Times*, 8 Apr. 2009.
- ¹⁹ At Foreign Affairs Committee Field Hearing, Berman Launches New Initiative to Fight Global Intellectual Property Theft, press release (Apr. 6, 2009), http://foreignaffairs.house.gov/press_display.asp?id=608.
- ²⁰ *Id.*
- ²¹ See Anne Broache, MPAA Wants ISP Help in Online Piracy Fight, CNET NEWS, Sept. 18, 2007, http://news.cnet.com/8301-10784_3-9780401-7.html.
- ²² 17 U.S.C. §§ 101–122 (2008).
- ²³ 17 U.S.C. §§ 102(a), 106.
- ²⁴ 464 U.S. 417 (1984).
- ²⁵ *Id.* at 442.
- ²⁶ 545 U.S. 913 (2005).
- ²⁷ *Id.* at 919–20.
- ²⁸ *Id.* at 934.
- ²⁹ *Id.* at 919.
- ³⁰ See 17 U.S.C. § 502 (2008).
- ³¹ *Id.* § 503.
- ³² *Id.* § 504(b).
- ³³ *Id.* § 504(c)(1).
- ³⁴ *Id.* § 505.
- ³⁵ See 17 U.S.C. § 1201 (2008).
- ³⁶ *Id.* 1203(c).
- ³⁷ *Id.* 1204(a).
- ³⁸ Apple, Changes Coming to the iTunes Store, press release (6 Jan 2009), <http://www.apple.com/pr/library/2009/01/06itunes.html>.
- ³⁹ 17 U.S.C. § 512(a) (2008).
- ⁴⁰ *Id.*
- ⁴¹ *Id.* § 512(c).
- ⁴² *Id.* § 512(c)(1)(C).
- ⁴³ *Id.* § 512(c)(1)(A)(i)–(ii).
- ⁴⁴ *Id.* § 512(c)(1)(A)(iii).
- ⁴⁵ See *id.* § 512(c)(3).
- ⁴⁶ *Id.* The notice must also include contact information to the complaining party and a statement that the information in the notice is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. *Id.*
- ⁴⁷ *Id.* § 512(h).
- ⁴⁸ *Id.* § 512(h)(2).
- ⁴⁹ *Id.* § 512(h)(3), (5).
- ⁵⁰ Sarah McBride and Ethan Smith, Music Industry to Abandon Mass Suits, *The Wall Street Journal*, 19 Dec. 2008.
- ⁵¹ *Id.*

If you have any questions about this *Client Alert*, please contact one of the authors listed below or the Latham attorney with whom you normally consult:

France – EU

Laurent Szuskin

+33.1.40.62.23.28
laurent.szuskin@lw.com
Paris

Sophie Fourques de Ruyter

+33.1.40.62.23.69
sophie.fourquesderuyter@lw.com
Paris

Jennifer Doucleff

+33.1.40.62.21.12
jennifer.doucleff@lw.com
Paris

Germany

Ulrich Wuermeling

+49.69.6062.6502
ulrich.wuermeling@lw.com
Frankfurt

United Kingdom

Larry Cohen

+44.20.7710.4735
larry.cohen@lw.com
London

Anne Ferris

+44.20.7710.4794
anne.ferris@lw.com
London

United States

Roxanne Christ

+1.213.891.8300
roxanne.christ@lw.com
Los Angeles

Peter Jasinski

+1.213.891.8180
peter.jasinski@lw.com
Los Angeles

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the attorney whom you normally consult. A complete list of our *Client Alerts* can be found on our Web site at www.lw.com.

If you wish to update your contact details or customise the information you receive from Latham & Watkins, please visit www.lw.com/LathamMail.aspx to subscribe to our global client mailings program.

Abu Dhabi

Barcelona

Brussels

Chicago

Doha

Dubai

Frankfurt

Hamburg

Hong Kong

London

Los Angeles

Madrid

Milan

Moscow

Munich

New Jersey

New York

Orange County

Paris

Rome

San Diego

San Francisco

Shanghai

Silicon Valley

Singapore

Tokyo

Washington, D.C.