crowell moring

CLIENT ALERT

European TMT & Privacy Bulletin - March 2013

Mar.28.2013

Sections of this issue:

ISP LIABILITY AND MEDIA LAW

"New public" and "New Technical Means" – Cumulative Criteria?

In its judgment of 7 March 2013, the Court of Justice of the European Union (CJEU) has confirmed that the retransmission over the internet of television broadcasts is a "communication to the public" within the meaning of Article 3 (1) of the Information Society Directive (Directive 2001/29/EC) requiring the consent of the relevant copyright owners even when this retransmission is only accessible within the broadcaster's initial catchment area.

Background

The judgment was issued following a preliminary reference made in proceedings between several UK broadcasters, ("the Broadcasters"), and TV Catchup Ltd ("TVC"), concerning the retransmission by TVC over the internet, substantially in real time, of the television broadcasts of the Broadcasters.

The Broadcasters are commercial television broadcasters who own copyrights in their television broadcasts and in films and other items which are included in their broadcasts. TVC offers an internet television broadcasting service permitting its users to receive, via the internet, 'live' streams of free-to-air television broadcasts, including the television broadcasts of the Broadcasters.

TVC ensures that those using its service can obtain access only to content which they are legally entitled to watch in the United Kingdom by virtue of their television license. Each subscriber receives its own stream from TVC.

The Broadcasters have instituted proceedings against TVC for copyright infringement, alleging that TVC's service infringes their exclusive right to authorize a "communication to the public" of their broadcasts. TVC argued that its service does not constitute a "communication". This argument was based on several CJEU cases, including *SGAE* Case C-306/05, *FAPL* Joined Cases C-403/08 and C-429/08 and *AIRFIELD* Joined Cases C-431/09 and C-432/09 according to which mere "*technical means to ensure or improve reception of terrestrial television broadcast to its catchment area*" do not constitute a communication. TVC's second argument was that its communication was not to the "public" since the online streams were only accessible to recipients located within the broadcasters' initial catchment area. Accordingly, the 'communication' was not addressed to a "new" public, not considered by the authors when they authorized the broadcast in question.

The Judgment

Preliminary Observation

The CJEU first reiterated that the principal objective of the Information Society Directive is to establish a high level of protection of authors, allowing them to obtain an appropriate reward for the use of their works, including on the occasion of communications to the public. This means that the phrase "communication to the public" must be interpreted broadly.

Communication

Given that the retransmission of a terrestrial television broadcast over the internet uses a specific technical means different from that of the original communication, the CJEU held that such retransmission must be considered to be a 'communication' within the meaning of Article 3(1) of the Information Society Directive. Consequently, such a retransmission cannot be exempt from authorization by the authors of the retransmitted works when these are communicated to the public.

The CJEU rejected TVC's objection that it provided a mere "*technical means to ensure or improve reception of* " the broadcast in its catchment area. The intervention of TVC consists in a transmission of the protected works at issue which is different from that of the Broadcaster. It is in no way intended to maintain or improve the quality of the transmission by the Broadcaster. Hence, it is not a 'mere technical means'

To the Public

The CJEU reiterated that the term "public" refers to "*an indeterminate number of potential recipients and implies, moreover, a fairly large number of persons*." That public can be determined by looking at the cumulative effect of making the works available to potential recipients i.e. the number of users who can access the service successively, as well as simultaneously. The CJEU also repeated that the fact that the potential recipients access the communicated works through a one-to-one connection is irrelevant. That technique does not prevent a large number of persons having access to the same work at the same time.

In the case at hand, the retransmission of the works over the internet was aimed at all persons resident in the United Kingdom who have an internet connection and who claim to hold a UK television license. Those people may access the protected works at the same time, in the context of the 'live streaming' of television programs on the internet.

The retransmission in question was thus aimed at an indeterminate number of potential recipients and implies a large number of persons.

In respect of TVC's objection based on the criterion of a "new public," the CJEU held that the situations examined in the cases which gave rise to the judgments in *SGAE, FAPL* and *Airfield*, differ clearly from the situation at issue in the case at hand. Those cases concerned situations in which an operator had made accessible, by its deliberate intervention, a broadcast containing protected works to a new public which was not considered by the authors concerned when they authorized the broadcast in question. By contrast, the case at hand concerned the transmission of works included in a terrestrial broadcast and the making available of those works over the internet. Each of those two transmissions must be authorized individually and separately by the authors concerned, since each of them is made under specific technical conditions, using a different means of transmission for the protected works, and each is intended for a public. The CJEU found that in those circumstances, it is no longer necessary to examine the requirement that there must be a new public.

Conclusion

The Court's ruling seems to suggest that the copyright owner's exclusive rights in "communications to the public" allow it to control both the technical means of transmission to the public and the public to which it is addressed. This would imply that as from the moment either the technical means or the public are "new," the copyright owner's consent would be required.

For more information, contact: Sofie Cubitt

ELECTRONIC COMMUNICATIONS & IT

ICANN Publishes Target Date For the Delegation of the First New gTLD

The policy for introducing new generic top level domains (gTLDs) or domain name extensions was approved by the ICANN Board on 20 June 2011. Over 1.900 applications for operating new gTLDs were timely submitted to ICANN and about 1.200 new gTLDs may be introduced. At present, ICANN is evaluating all gTLD applications. According to ICANN's latest information, the first new gTLD may go live later this year.

Background

In the past, ICANN has often been criticized for not being able to comply with self-imposed deadlines and target dates. In connection to the introduction of new gTLDs, the community long feared that the process would suffer further delays, because of ongoing discussions about the implementation and set-up of mandatory rights protection mechanisms.

New gTLDs to be expected soon

On 13 February 2013, ICANN provided for the first time a specific date on which it expects to be ready. ICANN's CEO said in an interview that ICANN expects to be able to recommend for delegation the first new gTLD on 23 April 2013. As from that date, new gTLDs will be delegated using a phased approach.

This announcement came as a surprise to the community, as ICANN had not yet given any indication that the mandatory rights protection mechanisms would be timely implemented. Shortly after the communication of 13 February 2013, ICANN and providers of rights protection mechanisms commented on the progress made in this respect (*See the Article on New tool to combat cybersquatting ready for implementation and the Article about the Trademark Clearinghouse that is about to launch in this newsletter)*.

It remains important to note that the recommendation for delegation does not mean that the gTLD will go live on 23 April 2013. The go-live date will depend on the Applicant's readiness and marketing plan. However, we would not be surprised that the first gTLD applicant who gets delegated the gTLD will make use of the momentum and launch the gTLD shortly after 23 April 2013.

Conclusion

As the introduction of new gTLDs may be expected soon, companies who want to register domain names in new gTLDs should prepare themselves to analyze the registration policies of this first new gTLDs and assess how they can claim rights in these new extensions.

For more information, contact: Jan Janssen

ELECTRONIC COMMUNICATIONS & IT

New Tool to Combat Cybersquatting Ready For Implementation

With the introduction of new gTLDs, ICANN will introduce new mandatory rights protections mechanisms. Among these mechanisms is the Uniform Rapid Suspension system (URS), which for a long time was considered to be a blocking factor to the introduction of new gTLDs. ICANN has now found a dispute resolution provider who is willing to offer URS services at the targeted pricing and finalized the rules governing the URS.

Background

The Uniform Rapid Suspension system ('URS') is a rights protection mechanism developed by ICANN to be implemented within new gTLDs that facilitates "rapid" suspension of domain names in clear-cut cases of trademark infringement. As ICANN has described the URS, It is intended to complement the existing Uniform Domain-Name Dispute Resolution Policy (UDRP) by offering a lower-cost, faster path to resolution for mark holders.

For a long period of time, the implementation of the URS was seen as a blocking factor to ICANN's new gTLD program as it seemed that the cost of the URS procedure as written would exceed targets. In September 2012, ICANN issued a Request for Information to find a candidate who would meet the requirements for providing URS services at the targeted cost.

ICANN Finds Dispute Resolution Provider and Finalizes the URS Procedure

On 20 February 2012, ICANN announced that it has appointed the National Arbitration Forum as the first of multiple providers that will be appointed to administer URS services. The process for appointing additional providers will be similar to that of appointing UDRP providers in which consideration is given to achieving competitive provisioning and geographical spread of providers.

Shortly after this announcement, on 5 March 2013, ICANN published a new version of the URS Procedure, a policy document updating the draft version of the policy that was posted in ICANN's June 2012 Applicant Guidebook. ICANN also published a set of Rules for the URS Procedure, similar to the Uniform Domain Name Dispute Resolution Policy (UDRP) rules. In addition to these Rules, each URS service provider is expected to produce supplemental rules to help standardize conduct for the prosecution of claims between complainants and respondents. Such supplemental rules must be in line with and may not contradict the URS procedure or the Rules.

With this updated version, the URS Procedure document now appears final.

In comparison with ICANN's previous draft, two changes are particularly relevant:

- A respondent, whether in default or not, will have 14 days from the date the decision (called Determination) is issued in order to file an appeal. In the previous version of the Procedure, a defaulting respondent was still able to seek relief from Default by filing a Response within 6 months of issuance of the initial Determination. This possibility is now excluded.

- A respondent shall pay a Response Fee if the Complaint lists 15 or more disputed domain names registered by the same registrant, instead of 26 or more according to the previous version of the Procedure.

Other changes to the Procedure appear largely cosmetic in nature.

The updated URS procedure contains no explicit reference to the approximate fee for URS proceedings anymore. The fee will need to be determined by the URS service providers. The Memorandum of Understanding between the NAF and ICANN provides that URS services will be provided on a reasonable and cost effective basis. The fee is expected to be between 300 and 500 USD.

Conclusion

The appointment of a service provider for the URS and the changes to the URS procedure are good news for trademark holders who wish to act rapidly against clear-cut trademark abuse in new gTLDs. Particularly in cases involving a high number of domain names, the URS may prove to be efficient in combating cybersquatters.

For more information, contact: Jan Janssen

ELECTRONIC COMMUNICATIONS & IT

Companies May Begin to Protect Their Online Presence Anew: Trademark Clearinghouse for New gTLDs Launched on 26 March 2013

As part of the new gTLD program, ICANN has introduced the Trademark Clearinghouse (TMCH). The TMCH will become a central repository of trademark related data that is used to support and streamline some of the mandatory rights protection mechanisms in new gTLDs. The TMCH has launched on 26 March 2013.

The purpose of the Trademark Clearinghouse

The Trademark Clearinghouse (TMCH) aims at providing trademark holders with more extensive and cost-effective opportunities to protect and safeguard their trademarks in the new gTLDs.

Starting on 26 March 2013, the TMCH will validate trademarks, which will allow trademark holders to participate in "Sunrise Phases" of the New gTLDs or to benefit from the so-called "Trademark Claims Service. A "Sunrise Phase" is a period of time before domain names become generally available to all eligible registrants during which trademark holders (who meet certain eligibility requirements) will be given the opportunity to register or block domain names corresponding to their validated trademark. The "Trademark Claims Service" is a system in which (i) a prospective registrant of a domain name will be provided notice of the existence and the scope of a validated trademark that corresponds to the requested domain name and (ii) the

holders of a validated trademark will receive a notification that a domain name that corresponds to their reported trademark has been registered.

The Main Working principles of the Trademark Clearinghouse

The main working principles of the TMCH are established in a Policy that is published in ICANN's Applicant Guidebook and the TMCH Validation Terms and Conditions (T&C's).

The TMCH service provider published the T&C's on 7 March 2013. These will apply as from the launch of the TMCH, on 26 March 2013. The TMCH service provider also published guidelines that provide an overview of the eligibility requirements and explain the types of marks that may be accepted for inclusion in the TMCH.

Ambiguity About Combined Marks

In the guidelines, it is described how combined marks (word + design) will be validated by the TMCH. However, the current version of the ICANN's TMCH Policy containing the eligibility requirements only mentions word marks for protection via the TMCH. This seems contradictory, and as the guidelines are supplementary in nature, the eligibility requirements contained in the TMCH Policy should prevail.
Then why do the guidelines refer to combined marks?

The fact that the TMCH may support additional protection mechanisms at the request of individual registries may explain this. The TMCH could indeed validate combined marks for those gTLDs who want to allow Sunrise registration based on a combined mark.

Another possibility is that the TMCH Policy will be modified going forward. The T&C's refer to the eligibility requirements for inclusion in the TMCH as specified by ICANN 'from time to time.' The acceptance of combined marks may be a welcome change for brand holders wishing to protect their combined marks in New gTLDs.

With a view to providing legal certainty, we can only hope that ICANN provides clarification in this respect sufficiently in advance of the first new gTLD going live.

For more information, contact: Jan Janssen

PRIVACY & DATA PROTECTION

Apps on Smart Devices and Data Protection: February 27, 2013 Opinion of the Article 29 Working Party Provides Valuable Guidance

Apps on mobile devices collect large quantities of data from the device and process these (i) in order to provide services to the end-user, but also (ii) for other purposes that are often unknown or unwanted by the end-user. Many of the data processed, such as location data, contact data, unique device and customer identifiers, credit card and payment data, browsing history, pictures, videos, etc., are personal data under EU data protection laws.

The various parties involved in the development and commercialization of mobile apps (or other mobile applications) are often unaware of their obligations under data protection law. These parties include app developers, app owners, app stores, operating system and device manufacturers and other third parties that may be involved in the collection and processing of personal data from smart devices.

In its opinion of February 27, 2013, the Article 29 Working Party[1] therefore tries to clarify the legal framework that applies to this processing and to clarify the responsibilities of all parties involved in the app development and commercialization process.

The Opinion identifies the most important data protection risks associated with mobile apps. It provides valuable guidance on *inter alia* the determination of applicable law. In this context, it is important to underline that the EU rules apply to any app targeted to app users within the EU, *regardless of the location of the app developer or app store.*

The Opinion underlines that privacy compliance should be implemented as from the development stage and by all parties involved. It is therefore advisable to *inter alia* contractually agree on the allocation of responsibilities, including the responsibility for technical and organizational security measures. The Opinion states that parties *have to take into account the principles of privacy by design and privacy by default*. This is clearly inspired by the obligations which will enter into force under the upcoming new EU Data Protection Regulation, discussed in our previous newsletters.

The Opinion provides examples of what constitutes personal data and sets out legal requirements for all parties involved.

Section 4 of the Opinion ("conclusions and recommendations") is particularly interesting, as it provides for a separate list of obligations (under the current Data Protection Directive and the e-Privacy Directive) and recommendations for each party involved.

For instance, with respect to *app developers*, the Opinion states the following:

App developers must

- Be aware of, and comply with, their obligations as data controllers when they process personal data from and about users;
- Be aware of, and comply with, their obligations as data controllers when they contract with data processors such as if they outsource the collection and processing of personal data to developers, programmers and for example cloud storage providers;

- Ask for consent before the app starts to retrieve or place information on the device, i.e., before installation of the app. Such consent has to be freely given, specific and informed;
- Ask for granular consent for each type of data the app will access; at least for the categories Location, Contacts, Unique Device Identifier, Identity of the data subject, Identity of the phone, Credit card and payment data, Telephony and SMS, Browsing history, Email, Social networks credentials and Biometrics;
- Be aware that consent does not legitimize excessive or disproportionate data processing;
- Provide well-defined and comprehensible purposes of the data processing in advance to installation of the app, and not change these purposes without renewed consent; provide comprehensive information if the data will be used for third party purposes, such as advertising or analytics;
- Allow users to revoke their consent and uninstall the app, and delete data where appropriate;
- Respect the principle of data minimization and only collect those data that are strictly necessary to perform the desired functionality;
- Take the necessary organizational and technical measures to ensure the protection of the personal data they process, at all stages of the design and implementation of the app (privacy by design);
- Provide a single point of contact for the users of the app;
- Provide a readable, understandable and easily accessible privacy policy, which at a minimum informs users about:
    - who the app developers are (identity and contact details),
    - what precise categories of personal data the app wants to collect and process,
    - why the data processing is necessary (for what precise purposes),
    - whether data will be disclosed to third parties (not just a generic but a specific description to whom the data will be disclosed),
    - what rights users have in terms of withdrawal of consent and deletion of data;
- Enable app users to exercise their rights of access, rectification, erasure and their right to object to data processing and inform them about the existence of these mechanisms;
- Define a reasonable retention period for data collected with the app and predefine a period of inactivity after which the account will be treated as expired;
- With regard to apps aimed at children: pay attention to the age limit defining children or minors in national legislation, choose the most restrictive data processing approach in full respect of the principles of data minimization and purpose limitation, refrain from processing children's data for behavioral advertising purposes, either directly or indirectly and refrain from collecting data through the children about their relatives and/or friends.

The Working Party <u>recommends</u> that app developers

- Study the relevant guidelines with regard to specific security risks and measures;
- Proactively inform users about personal data breaches along the lines of the requirements of the ePrivacy Directive;
- Inform users about their proportionality considerations for the types of data collected or accessed on the device, the retention periods of the data and the applied security measures;
- Develop tools to enable users to customize retention periods for their personal data based on their specific preferences and contexts, rather than offering pre-defined retention terms;
- Include information in their privacy policy dedicated to European users;

- Develop and implement simple but secure online access tools for users, without collecting additional excessive personal data;
- Together with the OS and device manufacturers and app stores use their creative talent to develop innovative solutions to adequately inform users on mobile devices, for example through a system of layered information notices combined with meaningful icons.

The full text of the Opinion can be found here.

---

[1] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

For more information, contact: Frederik Van Remoortel

CONTRACTS & E-COMMERCE

Belgian Regulator Fines Telecom Operators For Breach of Consumer Transparency Obligations

On January 31, 2013, the Belgian telecom regulator "BIPT/IBPT" fined three Belgian telecom operators for breach of certain consumer transparency obligations.

Background

In accordance with article 110 §4 of the Belgian Act on Electronic Communication ("AEC"), operators are required to inform subscribers at least once a year via their invoice about the most beneficial tariff plan taking into account their personal profile.

Article 4 of the Ministerial Decree of November 12, 2009 ("MB"), reads that operators must mention the expiry date of their contract on the subscriber's invoice if their contract is of definite duration.

In 2011, the Belgian regulator conducted an investigation into the compliance by Belgian operators with these provisions. Eighteen operators were asked to produce at random a number of invoices.

On the basis of these invoices, the BIPT/IBPT withheld a violation by Telenet and Mobistar of article 110 §4 AEC and a violation by Scarlet of article 4 MB. In its decisions of January 31, 2013, the regulator imposed a fine of 30,000 EUR. on Telenet and Mobistar and of 10,000 EUR. on Scarlet.

The regulator's application of article 110 §4 AEC and article 4 MB

The BIPT/IBPT's decisions of January 31, 2013, confirm that the regulator believes that article 110 §4 AEC and article 4 MB are not contrary to the European regulatory framework for the sector of electronic communications.

Although the Belgian legislator decided to go further than the transparency obligations imposed by the European framework, and in particular by EU Directive 2002/22 (Universal Service Directive), the BIPT/IBPT refers to the principle of minimum harmonization by the Universal Service Directive as confirmed by the CJEU in cases C-522/08 and C-543/09, and in article 1.4 of the Universal Service Directive.

Secondly, the regulator considers the transparency obligations of article 110 §4 and article 4 as "obligations of result" and applies them in a strict manner.

In this regard, the regulator finds it insufficient that the operators included an explicit statement on their invoices referring the consumer to a specific webpage or to the customer service and/or to a specific tariff check service to obtain more information on the most advantageous tariff plan given his profile.

Given the wording of article 110 §4, operators must provide this information to the subscriber *on the invoice* and the subscriber should not be required to take any particular action to access this information (such as visiting a website). The regulator refers to a similar reasoning held by the CJEU in its judgment of July 5, 2012 with respect to the information obligations in the framework of distance contracts (case C-49/11).

The regulator's strict interpretation was also confirmed in its decision towards Scarlet, in which BIPT/IBPT imposed a fine even though only 4 out of 40 invoices did not include the reference to the expiry date required by article 4 MB.

For more information, contact: Karel Janssens

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Thomas De Meese
Partner – Brussels
Phone: +32.2.282.1842
Email: tdemeese@crowell.com

Frederik Van Remoortel
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com