e-commercelaw&policy

THE E-COMMERCE NEWSLETTER FOR ONLINE BUSINESS
FEBRUARY 2013 VOLUME 15 ISSUE 02 **WWW.E-COMLAW.COM**

FTC issues mobile privacy staff report

The FTC issued a staff report on 1 February providing recommendations for companies to improve mobile privacy disclosures. "The report represents a culmination of efforts initiated by the FTC and other regulators during the past few years," said Gonzalo Mon, Partner at Kelley Drye. "The FTC's perspective is that the report is necessary to achieve stronger enforcement of disclosure standards for apps," adds John Feldman, Partner at Reed Smith.

"The report contains four recommendations," said Mark Brennan, Associate at Hogan Lovells, "(1) have a privacy policy and make it available prior to download; (2) provide 'just-in-time' disclosures and obtain affirmative express consent when collecting sensitive information outside the API; (3) improve coordination with advertising networks and third parties; and (4) consider self-regulatory programs."

The report accompanied the FTC's settlement against the Path social networking app, which allegedly collected PI from users without their knowledge or consent. "App developers should say what they do," concludes Mon, "and do what they say."

IN THIS ISSUE

News Aggregation Dispute **03**
Internet Tax The Colin & Collin Report **06**
File-Sharing Monitoring BitTorrent **08**
Cybercrime Changes in Singapore **10**
Online Advertising Germany **13**
Hyperlinks Legality **14**
Case Law Update **16**

French report proposes to tax online data collection

The French government released on 18 January a report proposing changes to international tax rules to better account for value creation by digital firms, recommending an online tax based on data collection.

"With respect to international taxation, e-commerce companies are advantaged compared to other industries needing a local presence to carry out their business activity," said Julien Monsenego and Rui Cabrita of Olswang. "However, the rationale behind the report relies on the idea that in e-commerce user data is a key resource. The authors seem to present user data as a cause of profitability not a consequence. One can argue that the profitability of these companies is derived from their ability to meet the needs of their audience."

The report authored by Colin and Collin was commissioned in July 2012 by the French government. "According to the report, companies which carry out 'regular and systematic monitoring of data' provided for free by their users would be subject to taxation," said Guilhem Calzas, Associate at Bignon Lebray. "Companies would have to declare the amount of data they collect and the rate adjusted depending on whether the company abides by data protection regulations."

"The report seeks to justify the tax on the basis that users are, in effect, working for free in providing the information," said Vanessa Barnett, Partner at Charles Russell. "The application of the tax will depend on the number of users located in France whose data is used," adds Nathalie Dreyfus, Founder of Dreyfus & Associés. "The material and territorial scope suggested for the tax would cover all companies regardless of their State of establishment."

The report acknowledges that such a tax depends on international support for its success. "Achieving a change in the definition of the permanent establishment concept leads to a renegotiation of existing tax treaties," said Philippe Lorentz, Partner at August & Debouzy Avocats. "A review of the transfer pricing criteria has also been proposed to better allocate taxable income between the States. In the meantime and due to the fact that such proposals take time, it is proposed to apply a specific tax based on the exploitation of user data."

"OECD is currently involved in the Base Erosion and Profit Shifting project aimed at assessing if the current rules allow the allocation of profits in a place different to where the business activity is carried out," adds Mosenego. "The next G20 summit could be the occasion for guidelines on the issue."

FFIEC issues rules for financial institutions on social media

The Federal Financial Institutions Examination Council (FFIEC) proposed on 22 January guidelines for financial institutions interacting on social media, to ensure banks comply with regulations and protect consumers.

"Institutions are becoming increasingly active on social media, but there are many unknowns," said Nicole Muryn, Director of Legislative and Regulatory Affairs at BITS. "For example, how does a Facebook 'like' compare with an endorsement? The guidelines will help institutions understand how regulators view these issues."

The FFIEC highlights the need to comply with regulations regarding marketing on social media. "The informality and real-time nature of many social media types are in tension with the careful vetting generally needed for communications to the public governed by financial services laws and regulations," said Andrew Lorentz, Partner at Davis Wright Tremaine.

The FFIEC recommends institutions implement an oversight system to monitor the content posted on social media, though Lorentz believes this would likely only "create another box to check off" and explains "Social media calls for rigorous management, but that is the 'business as usual' expectation for financial institutions."

Mark Johnson, Founder of the Risk Management Group, believes that to be "truly effective," policies must "address the wider issues related to employee behaviour in the personal social media space. The proposals are a welcome starting point, but cannot be the whole story."

ecommercelaw&policy

THE E-COMMERCE NEWSLETTER FOR ONLINE BUSINESS
VOLUME 15 ISSUE 02 FEBRUARY 2013
WWW.E-COMLAW.COM

Editorial: Song-Beverly Act

The balance between adequate protection of consumer data and the need for companies to acquire such data from their customers in order to ensure consumer safety has been examined recently by the California Supreme Court, in Apple Inc. v. Sup. Ct. of Los Angeles County. The case was brought to the Court by plaintiff David Krescent, who took issue when major e-retailer Apple required his phone number and address before accepting his credit card payment for electronic goods online.

This case turned on the interpretation of California's Song-Beverly Credit Card Act. This legislation from 1971 pre-dates the popular use of the net and forbids retailers to acquire a consumer's personally identifying information (PII) as part of accepting an individual's credit card for payment; Krescent's opinion was that Apple's card requirements placed it in violation of the Act. Apple's argument was that the information asked for is necessary: if online retailers cannot verify a cardholder's identity, the risk of fraud is increased.

The Supreme Court found in Apple's favour by a majority of 4-3. The Court ruled that the Song-Beverly Act, although its text is indecisive around the issue of e-commerce specifically, was not designed to leave either retailer or consumer vulnerable to fraudulent practice. Since online retailers selling products via electronic download struggle to offer the extent of protection against fraud as those in bricks-and-mortar stores, the Act does not apply in these cases.

The Court was selective in its verdict, however. The ruling holds only that the Act does not apply to electronic goods purchased online - so other goods bought on the internet are not covered. There is plenty to suggest that this issue is far from over, too. Dissenting judges expressed concerns about how much consumer information is collected online and about its later uses. The Court's comments imply that there is room for this issue to be further examined by lawmakers.

Simon Fuller

We are delighted to welcome Michelle Cohen, Member at Ifrah Law, to the Editorial Board.

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Associate Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Editorial Assistant Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions David Guati
david.guati@e-comlaw.com
telephone +44 (0)20 7012 1387
Design MadeInEarnest
www.madeinearnest.com

E-Commerce Law & Policy
is published monthly by
Cecile Park Publishing Limited
17 The Timber Yard, Drysdale Street,
London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093
www.e-comlaw.com

Online news aggregation services: the dispute

News aggregation services provided by internet search engines were once considered promotional tools for digital versions of traditional newspapers; however, more recently publishers have altered their views. Many news publishers now believe that services that collate news stories actually divert traffic away from the source story. Some go further and claim that news aggregators infringe the publishers' copyright. Yet search engine owners argue that such aggregating services are useful for publishers, providing them with much needed traffic. Farah Mukaddam, of Norton Rose, explores the legal background to this debate and the approaches to settling the dispute.

There is a storm brewing between news publishers and internet search engines over the way in which search engines collate and present news stories from various online sources. Despite initial fears that the internet sounded the death knell of traditional newspapers, many newspapers have developed successful online businesses. The New York Times and the UK's Daily Mail both have websites that rank in the top 150 sites in the world, each boasting over 70 million unique users a month. However, a new threat has emerged in the form of news aggregation services provided by internet search engines such as Google News and Bing News from Microsoft.

These services collate the most popular news stories from around the world, summarising copy from authoritative news sources with references and links to the original source. The issue for news publishers is that the appetite of time-starved consumers for news is sated by these summaries. The result, say the news publishers, is a reduction in the number of visitors to their websites. Consequently these news publishers are unable to successfully monetise their endeavour in creating these stories through online advertising. Given that display advertising is fast becoming the main source of revenue for online news publishers, this could become a major issue for the long term viability of these services. The news publishers argue that such use of their content amounts to copyright infringement.

Obviously this is only one side of the story. Leading the rebuttal on behalf of the search engines is Google. Google has recently settled two court actions brought by French news agency Agence France-Presse and the Belgian news agency Copiepresse. The actions were for copyright infringement of headlines and snippets of news articles/wires and photos used in Google News. Google's defence is that its use is for the purpose of news reporting which constitutes fair use and renders it non-infringing. Google also say that Google News results in billions of click-throughs to news sites around the world, i.e. rather than undermining news publishers, Google News actually increases traffic to the sites originating the articles by referring to them in a way that is more meaningful and accessible to web users. Google News is not currently monetised by Google as it is subscription-free and does not feature any advertising on its pages.

The furore has come to a head in Europe where news publishers are gathering political momentum by lobbying governments, notably in Germany and France. The news publishers are asking for amendments to long established copyright laws, extending the scope of copyright protection to cover headlines and excerpts of news articles that appear in search results, and want to introduce a levy for use of the content in aggregating news services. Whether this will provide the answer that news publishers and search engines are looking for remains to be seen.

Is aggregation of news headlines permitted by law?

The dispute is by no means clear cut. This may explain the lack of serious litigation to date.

Essentially the legal argument turns on whether the use of headlines and snippets of news articles amounts to copyright infringement or whether such activity is a permitted act on the basis of 'fair use' exceptions.

Copyright

Original news articles which are

published on websites may be afforded literary copyright protection. Specifically, in the English case of The Newspaper Licensing Agency Ltd and others v. Meltwater Holding BV and others[1] (applying the European Court of Justice's decision in Infopaq International A/S v Danske Dagblades Forening[2]) the English Court of Appeal held that headlines and extracts of articles were capable of being recognised as literary works and so afforded copyright protection. In the Infopaq case the European Court of Justice ruled that eleven words of copying could amount to copyright infringement if what is copied represents an element of the work which expresses the author's own intellectual creation. The decision in Meltwater also indicates that the provision of a link to content could amount to copyright infringement where the link itself is capable of being afforded copyright protection (in the case the link was made up of the headline of the article).

These principles form the basis on which news publishers can argue that their content should be protected from use by aggregation services. Assuming that the news articles, headlines and extracts are copyrighted works, infringement may occur when Google performs the restricted acts of copying headlines and extracts and communicating them to the public as part of the Google News service. Further, assuming that the links are copyrighted works, infringement of the copyright in those links may occur when Google performs the restricted acts of reproducing those links and, possibly, of making the links available to the public (although the latter was not considered in Meltwater).

Fair use

As one would expect, Google claims to have a robust defence to these arguments. Again assuming that the news articles, headlines, extracts and links are copyrighted works, Google maintains that its use is non-infringing on the basis that use for the purpose of news reporting is regarded as fair use.

Some commentators have considered whether there may be an implied licence granted to Google for use of news content given the ease with which news publishers can ensure that their stories do not feature in Google News (by notifying Google or using a robots.txt file in accordance with instructions provided by Google[3]). However, it is debateable whether a copyright owner's inaction to prevent an infringing act should be defined as the grant of an implied licence. We note that news publishers in Brazil, accounting for 90% of Brazil's news circulation, have opted out of Google News (although their withdrawal does not stop their content from coming up in general search results). News publishers could prevent Google's use of their content by putting up paywalls and/or requiring a log-in to access content as services such as The Times have already undertaken. This does however involve a significant shift in the overall business model. Given the news publishers' inaction, it may well be a safe assumption that news publishers are benefiting from referrals gained from aggregation services like Google News.

Given the veracity of the arguments on both sides, commencing litigation seems to be a risky strategy; this may explain the lobbying of governments instead.

Legislative proposals

News publishers throughout Europe have been putting pressure on governments to intervene in the debate and introduce an extension to copyright protection and/or a tax on search engines for use of content at a national level. There have also been reports of coordinating these efforts internationally. The lobbies in Germany and France have been particularly successful.

The German government has drafted a bill which would create a new form of ancillary copyright for news publishers which previously did not exist. This would give news publishers the exclusive right to make their works publicly available for commercial purposes and search engines would be required to pay for use of the content for a year after publication. The legal committee of the Bundestag scheduled a public hearing for 30 January 2013, suggesting that plans to introduce the law in 2013 are moving steadily ahead.

In October 2012 the French president François Hollande met with Google's executive chairman. Hollande demanded that Google reach a deal with news publishers by the end of the year, threatening to draft legislation to require Google to pay a fee for linking to content if Google failed to strike a deal, following the German example.

Google opposes the proposals; it has threatened to stop linking to French news publishers' content if France was to introduce such legislation and has commenced a campaign calling for its users to protest against the proposals in Germany. Google has stated that the proposals would threaten its existence and be detrimental to freedom of information and communication on the internet. Other criticisms suggest the proposals would harm news publishers who benefit from traffic referred to them by Google and other aggregation services; that an adverse impact would be levied on

new market entrants who may not be able to pay the licence fees; and that difficulty in enforcing the legislation beyond national barriers makes the legislation unworkable.

Google's North Europe Communications Chief Kay Oberbeck commented on the current situation suggesting that 'Publishers should be innovative in order to be successful. A compulsory levy for commercial internet users means cross-subsidising publishers through other industries. This is not a sustainable solution.'[4] The argument is certainly persuasive; but what other options are there for resolving the dispute?

The AFP and Copiepresse approach

In 2005 Agence France-Presse, a global news agency that licenses news stories to other news providers, sued Google for copyright infringement for use of its copyrighted wire stories and photos in Google News. Agence France-Presse argued that only licensed parties were authorised to publish the content and by providing the content, even in an abbreviated form, Google was infringing its copyright. After two years of litigation, the parties settled by entering into a licensing deal enabling Google to use Agence France-Presse's content in its Google News service; details as to the terms of the settlement deal were not disclosed.

Similarly in 2006, Copiepresse, an agency acting for Belgium's French language news publishers, sued Google for copyright infringement for use of headlines and snippets of articles in Google News and linking to cached copies of their work in the general search. On appeal the court upheld the decision of the first instance court in Copiepresse's favour and ordered Google to remove the links.

Rather than looking to governments to change well-established copyright laws in order to protect revenues in a fast changing digital environment, it is suggested that news publishers look to find other commercial solutions to protect and possibly increase their revenues.

Despite the court's ruling, the parties reached an agreement last month. They will partner together on a range of initiatives to take advantage of each other's advertising platforms amongst other things. The deal will see Google commit to advertising in Belgium's French language newspapers and Belgium's French language newspapers commit to using AdWords and other Google platforms to attract new readers. Google also plans to implement official YouTube channels on news publishers' websites and push use of mobile devices to distribute content. Google agreed to pay all of Copiepresse's legal fees, although the amount was not disclosed.

In the face of the deal, Google has been careful to reiterate its position that it has not infringed copyright and that the deal does not amount to a tax for use of content. There may however be some strength to the argument that Google's commitment to advertise on Copiepresse's website (and Google's payment of Copiepresse's legal fees) amounts to avoidance of a direct copyright levy.

News aggregation 2.0

Rather than looking to governments to change well-established copyright laws in order to protect revenues in a fast changing digital environment, it is suggested that news publishers look to find other commercial solutions to protect and possibly increase their revenues from this activity. News publishers need only take heed of the perils of over reliance on legislation that befell the music industry. The shutdown of the original Napster peer-to-peer file-sharing internet service following claims for copyright infringement by the music industry in 2000 is particularly pertinent. The closure of the service lead to a proliferation of other online music file sharing services. Had the music industry sought a commercial deal to partner with the original Napster and embrace the benefits of new technology to its consumers, rather than seeking to shut it down, the music industry might conceivably have benefited from the service's dedicated user base and reduced online piracy in one stroke. Instead, many years of costly litigation and lobbying of governments later, the music industry is in arguably a worse position than it was pre-shut down of the original Napster. Online news publishers should be careful not to end up in the same situation. Using legislation to prevent usage of news extracts could alienate users who benefit from services such as Google News. Inevitably new services will also emerge that either avoid the new legislation or shamelessly infringe copyright in the news articles in the name of consumer demand. Stopping these services from operating would be a costly and time-consuming affair.

Instead, it may well be more sensible for news publishers to get on with the process of digitisation and strike commercial deals with Google and other search engines to adequately monetise the use of extracts, creating an additional revenue source for news publishers, rather than to persist with lobbying for legislative changes and claims for copyright infringement.

Farah Mukaddam Associate
Norton Rose
farah.mukaddam@nortonrose.com

1. [2011] EWCA Civ 890.
2. (Case C_5/08).
3. http://support.google.com/news/publisher/bin/answer.py?hl=en&answer=94003
4. http://gigaom.com/europe/google-lashes-out-at-german-copyright-threat/

How to tax the internet: the French Colin & Collin report

The question of how to obtain a greater amount of tax from big internet companies - such as Google and Amazon - is one that is currently perplexing many governments. In France, the recent Colin & Collin report explores how the tax avoidance practices of internet giants can be reversed, and puts forward the idea of a data tax, which would require online companies to pay for their use of user data. Jérôme Granotier and Guilhem Calzas, of Bignon Lebray Avocats, analyse the report's findings and what such a data tax would involve.

For many years, the French government has been concerned with the fact that internet giants, such as Google, Apple, Facebook and Amazon (the 'GAFA'), pay very few taxes in France. The business models of these companies mainly rely on the exploitation of data generated by their users, many of whom live in France. Yet, this exploitation of data is currently not taxed in France.

For instance, Amazon uses the comments published by its users in order to make personalised product suggestions to its other clients, which has been proven to significantly increase the company's sales. Thanks to well-planned tax optimisation strategies and the localisation of intellectual property assets in tax havens (e.g. Bermuda, in the case of Google), the billions generated by the internet giants are rarely subject to taxation in the countries where the people who are providing them with raw materials are living.

In order to tackle this issue, last summer the French government entrusted Mr. Nicolas Colin (Finance Inspector) and Mr. Pierre Collin (Councillor before the Administrative Supreme Court) with the task of finding a solution to levy taxes on companies which run their business exclusively online.

For Mr. Colin and Mr. Collin, who have just published their report, the best solution would be to levy corporate income tax on the business income generated by these companies. They admit, however, that current international and French tax laws have become obsolete and must be reformed before this can be done.

Based on the OECD model tax convention, international tax treaties provide that a State may only tax companies that have their headquarters located in its territory or that have a 'permanent establishment' there. A company is deemed to have a 'permanent establishment' in a State where it has a place of business, such as an office or a manufacturing plant, as well as permanent staff. However, when a company merely collects data from the people living in a given country, this country is not entitled to levy taxes on the company.

This taxation will only be possible if the concept of 'permanent establishment' is redefined. Within the framework of the G20 and the OECD, France will push forward to speed up the renegotiations of the tax treaties for this purpose. Still, the modification of tax treaties may take months, if not years, to be completed.

However, Mr. Colin and Mr. Collin warn that tax reforms are needed urgently to put an end to this 'deadly spiral.' As the internet giants benefit from the low tax rates of the tax havens, digital companies located in France face unfair competition and will progressively disappear. Google and Amazon, for instance, have already eliminated most of their competitors.

Moreover, data collection and processing no longer concern only digital companies. Data is also being collected by an increasing number of companies operating in more traditional industries, such as banking, tourism, telecommunications and health services. If tax optimisation through the use of tax havens continues to grow, the result will be a massive erosion of tax revenues and a negative affect on jobs in France, the reporters say.

In order to provide the French government with a short-term solution, Mr. Colin and Mr. Collin suggest introducing a new tax to which companies benefiting from the free provision of data by internet users living in France would be subject. The tax could be introduced by the 2014 Finance Law, i.e. as soon as January 2014.

According to the report, this taxation would be justified by the fact that the people who use the services provided by digital companies carry out 'free work' to the benefit of these companies. Data subjects are not only users, but also partners of digital companies. Indeed, thanks to data collected from individuals, companies are able to measure and improve their performance, and to provide their clients with more personalised services. Data can also be licensed for a fee to third parties, e.g. through software platforms.

The tax rate would hinge on the number of people who provide data to the company. The rate would also be adjusted depending on whether or not a particular company abides by French regulations relating to personal data protection. These regulations provide, for instance, that companies must inform internet users about the nature of the data

they have collected from them. They also provide for an obligation to quickly modify or return the data upon request of its data subject. In practice, a company that sets up, on its website, an interface allowing users to easily check, modify or delete the data collected from them would pay less tax. On the contrary, a company that purposely hinders users from accessing data collected from them would pay more tax.

Such taxes, designed to encourage or discourage certain types of behaviour among taxpayers, already exist, in particular in the field of environmental protection. For instance, eco-taxes based on the 'polluter pays principle' are already implemented in many countries, including France. However, as was the case with eco-taxes, the establishment of the new tax would raise a series of practical and legal issues.

First, the report does not clearly determine which companies would be subject to taxation. Mr. Colin and Mr. Collin state that only the companies which carry out a 'regular and systematic monitoring of data' provided for free by their users would be concerned. However, this rather vague concept, which has been introduced in a draft regulation of the European Parliament, has yet to be defined.

Moreover, it is still difficult to assess the value of users' personal data. Mr. Colin and Mr. Collin recognise that none of the economists they have met during their investigation have been able to provide them with a relevant formula to allocate income between the States where the digital companies are located and the States where their users live.

It is still difficult to assess the value of the users' personal data. Colin and Collin recognise that none of the economists they met during their investigation have been able to provide them with a relevant formula to allocate income between the States where the digital companies are located and the States where their users live.

In order to test the tax and to make any necessary adaptations before implementing it on a large-scale, the report suggests applying the new tax to a few companies first, as was done when VAT was implemented in France. These companies could be selected on the basis of different criteria.

One idea is to only tax companies which collect an amount of data above a determined threshold. This solution would have the advantage of preventing the business development of start-ups from being hampered by the tax. However, it would be difficult to draw a line between the companies which would be exempted from the tax and those which would have to pay it. The latter may question the validity of the tax in court on the basis of an infringement of the equality principle.

Another criterion could be to tax only the companies which have the status of 'hosting company.' However, and again, the French constitutional court may rule that this criterion is not directly linked to the purpose of the new tax, i.e. enforcing the protection of personal data. The argument would be that these companies do not infringe the regulations relating to personal data more than any other companies. Indeed, hosting companies are defined as those which lease servers on which their clients can store data.

One of the important points on which the report remains silent is that even if all of these issues are solved and the tax is successfully implemented, it may still be inefficient. Indeed, taxes designed as a deterrent usually generate little income for States, as taxpayers tend to adapt their behaviours in order to pay the minimum tax. In the end, companies located outside France will likely not pay more taxes than they do now.

For these reasons, the proposal for the new tax should be mainly considered as a starting point within the framework of international negotiations. Agreement on a common solution is the only way in which States will be able to hamper tax revenue erosion and profit shifting. As well as recommending that companies should be taxed in the countries where their data providers live, Mr. Colin and Mr. Collin provide the French government with legal and economic arguments for the implementation of this solution at a global level. There is no doubt that the taxation of digital companies will be one of the key issues discussed during the G20 summit in Moscow on 15-16 February.

Jérôme Granotier Partner
Guilhem Calzas Associate
Bignon Lebray
jgranotier@bignonlebray.com
gcalzas@bignonlebray.com

The full report (in French) is available on the website of the French Ministry of the Economy at the following address: http://www.redressement-productif.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf

BitTorrent tracking as a means of detecting illegal file-sharing

A recent academic study found that many organisations are now using online monitoring techniques to detect illegal file-sharing taking place through services such as BitTorrent. Tom Harding, a Senior Solicitor in Osborne Clarke's Digital Media team, discusses the study, and the extent to which monitoring evidence can potentially be relied upon in copyright infringement proceedings.

Birmingham academics Chothia, Cova et al recently published a study entitled 'The Unbearable Lightness of Monitoring; Direct Monitoring in BitTorrent.' It looks at the types of organisations monitoring illegal file-sharing and the methods they are using. It is well-known that this type of monitoring takes place. What the study tries to add to the debate is to delve deeper into the underlying techniques of the monitoring process itself and its prevalence.

Monitoring the monitors

As the study confirms, 'BitTorrent is widely used for the illegal exchange of copyrighted material, such as music, movies and software in particular, copyright holders are known to routinely monitor file-sharers, collect evidence of infringement, issue cease and desist letters and, in some cases, demand financial compensation.' This is nothing new, and previous cases have shown the difficulties that can arise from adopting a cease and desist/compensation approach. What the study claims to add however is a review of the 'precise techniques employed by enforcement agencies [in performing monitoring], which have never been disclosed publicly.' As a result, the researchers claim to have gathered evidence for the first time that enforcement agencies are now using 'direct monitoring' techniques to detect file-sharing.

The study's main focus is on the technical aspects of monitoring. The two types of monitoring identified are:

- 'indirect monitoring' - here, the monitor 'announces' itself to the relevant BitTorrent file 'trackers,' and in turn the tracker shares the IP addresses of users who have also 'announced' themselves. This technique offers a quick way of harvesting a large number of IP addresses of file-sharers, but offers no other evidence of potential involvement with any files they may be up/down loading; and
- 'direct monitoring' (either 'active' or 'passive') - the study claims to have gathered the 'first ever measurements' that enforcement agencies are now using this technique. Here, agencies 'establish connections with peers to estimate their participation in sharing activity.' In contrast to indirect monitoring therefore, direct monitoring looks to demonstrate that users are actually engaging in file sharing.

In addition, the researchers looked at the activities being monitored. They only found the presence of direct monitors in the 'Top 100' torrents, implying that 'copyright enforcement agencies are monitoring only the most popular content.' The study also found that 40% of monitors would be able to track illegal file-sharing within an average time of three hours.

Evidence matters

It is clear that illegal file-sharing is widely monitored. As a result, a lot of data is being collected, as lead researcher Tom Chothia was reported to have stated, however, 'Many firms are simply sitting on the data. Such monitoring is easy to do and the data is out there so they think that they may as well collect it as it may be valuable in the future.' This in itself raises data privacy issues but, those aside, also leads to arguably the key question - once a rights holder obtains monitoring data, what can it do with it? According to the study, in some cases 'direct monitoring... falls short of providing conclusive evidence of copyright infringement' and it questions whether solely relying on the evidence/techniques used would be enough to 'prove' a file was being shared. For present purposes, wider evidential issues associated with P2P file-sharing have been discussed in recent cases.

Case by case

Golden Eye Limited and others v. Telefónica UK Limited [2012] was a High Court case where various copyright owners were seeking a Norwich Pharmacal order against O2 'to obtain disclosure of the names and addresses of customers of O2 who are alleged to have committed infringements of copyright through peer-to-peer file-sharing using the BitTorrent Protocol.' In this case, the applicants had used 'Xtrack' software to identify uploaders/ 'seeders' of specific films and harvested the IP addresses of the alleged infringers.

The applicants were ultimately successful in gaining a Norwich Pharmacal Order, but during the hearing some of the issues associated with IP evidence were discussed. The backdrop to the discussion was that, as held by Mr Justice Arnold, 'it is not a requirement for the grant of Norwich Pharmacal relief that the applicant intend...to bring proceedings against the wrongdoer(s),' and that it was only required to establish that 'arguable wrongs' had been committed; in other words, the merits of any

subsequent infringement action were not required to be analysed in any detail as part of the proceedings. However, various issues associated with IP address evidence were highlighted including that 'It is technically possible, using appropriate monitoring or tracking software, to identify IP addresses which are participating in P2P file-sharing of particular files at particular times...[however,] even if the monitoring software is functioning correctly, ISPs sometimes misidentify the subscriber to whom the IP address which has been detected was allocated at the relevant time.' Further, even if the software is working correctly and the correct IP address has been identified, Mr Justice Arnold identified potential issues with this sort of evidence, including that:

- the IP address identifies a computer, but another person in the same household as the subscriber could be using the computer at the relevant time;
- the IP address identifies a router, but another person in the household may be using a different computer but on the same router;
- the IP address identifies a wireless router, but someone outside the household may have accessed this without the knowledge of the subscriber;
- the relevant router or computer was infected by a Trojan and someone outside the household was using the computer to access the internet; and
- the IP address identifies a computer open to public use.

Any of the above could be used to challenge whether IP address monitoring evidence alone would be robust enough to meet the 'balance of probabilities' test for successful infringement action.

The Media C.A.T. Limited v. Malcom Adams and Others [2011] EWPCC 6 case also covered similar ground. Media C.A.T. launched actions against various alleged infringers based upon BitTorrent tracking evidence. A discussion around the nature and robustness of this evidence arose. Judge Birss QC commented that "there is no dispute that P2P file-sharing software can be used to infringe copyright...but that can be said of many things. Proof that a person owns a photocopier does not prove they have committed acts of copyright infringement."

Although monitoring evidence can form part of the evidence presented in support of a copyright infringement claim, it seems it may not be enough by itself.

Judge Birss discussed the Polydor Limited and Others v. Brown and Others [2005] EWHC 3191 (Ch) summary judgment decision as an example of a successful infringement action against an individual resulting from their P2P file-sharing activity. Here, the defendant admitted to using P2P software, having control over the computer, but claimed he had been unaware that he was distributing music from his computer as a result. Polydor demonstrates that P2P file-sharing can ultimately be held to be an infringement (as was also more recently held in Dramatico Entertainment v. BskyB [2012] EWHC 268 (Ch)), but as Judge Birss pointed out in Media C.A.T., the mere use of P2P software itself was not enough to prove infringement.

Although monitoring evidence can form part of the evidence presented in support of a copyright infringement claim, it seems it may not be enough by itself. Of course, alongside litigation, rights holders may also have other routes of redress against alleged infringers under the Digital Economy Act - namely the sending of letters to suspected infringers by the ISP following receipt of a Copyright Infringement Report from a rights holder. We have not looked here at how tracking evidence links into the evidential requirements for these reports as the Initial Obligations Code has yet to be approved at EC level and laid before Parliament.

US developments

A US company, Malibu Media, LLC adopted a strategy of launching mass lawsuits for copyright infringement based on IP tracking evidence and is referenced in the study. Again, the aim seems to be to settle rather than go to full trial. However, Judge Michael Baylson raised issues with the initial evidence on the basis that 'a mere subscriber to an ISP is not necessarily a copyright infringer...there is no reason to assume an ISP subscriber is the same person who may be using BitTorrent to download the alleged copyrighted material.' As a result, the judge ordered that some of the actions go to full trial to establish the robustness of the evidence. As the same technologies apply across different jurisdictions, and the underlying evidential arguments are also likely to apply, any analysis may inform the debate in the English courts.

Conclusion

Monitoring of alleged file-sharing activity is no doubt increasing. Although the use of evidence gained from this will no doubt play a significant role in seeking to pursue alleged file-sharers, additional evidence is likely to be required for an action to be successful. That said, it seems that such evidence will in any event be valuable if seeking disclosure of alleged file-sharers' details from any intermediary via a Norwich Pharmacal order. Practice and technologies in this space are developing quickly, so further legal developments can also be expected.

Tom Harding Senior Solicitor
Osborne Clarke
Tom.Harding@osborneclarke.com

Singapore's Computer Misuse Act: updated cyber-defences

A recent amendment to Singapore's Computer Misuse Act is designed to enable a 'nimble and comprehensive response' to the threat of cyber-attacks. But some argue that the new Government powers are too broad and are open to abuse. Olswang Asia's Rob Bratby and Matt Pollins examine the key provisions of the new law and what it might mean for organisations in Singapore and beyond.

'Sophisticated and malicious.' 'A real and present danger.' 'A broad spectrum of attacks and threats.' These are not sensationalist headlines but comments from the Singapore Government's Second Reading Speech on the Computer Misuse (Amendment) Bill. The language used underlines the level of concern with which the Government views the threat of cyber-attacks. And the Singapore Government is not alone. With the recent high profile hack of the New York Times, and attacks like 'Stuxnet' and 'Flame' making the news and the World Economic Forum ranking cyber-attacks among the top five global risks, the issue is rapidly moving up the legislative agenda for governments around the world. As such, the new Singapore law could be a glimpse of things to come in other jurisdictions. So what are the key changes to the old legislation and what action might organisations be required to take?

New teeth

The headline provision of the new law is a broad right for the Singapore Government to compel action in the defence against cyber-attacks. Specifically, the Government can require any person or organisation to 'take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service or any class of computers or computer services.'

This power to compel a person or organisation to take action is the key change that the new law brings into effect. Under the previous legislation, the Government was only entitled to authorise a person or organisation to take action. The right to authorise was of course dependent on the relevant person or organisation actually electing to take the measures in question at its discretion. In short, the new law has teeth where the old law did not. But exactly what kinds of measures might organisations be required to take?

Proactive and reactive

The legislation is drafted broadly. The Government can require the taking of 'measures' and compliance with 'requirements.' The only condition is that the measures are 'as may be necessary to prevent, detect or counter any threat to a computer or computer service or any class of computers or computer services.'

The scope, therefore, is both proactive (to 'prevent') and reactive (to 'detect' and 'counter') and could potentially cover both offensive (whether pre-emptive or retaliatory) and defensive actions. But organisations will want to know what this could mean in practice. The legislation is quite helpful in this respect because it includes a non-exhaustive list of the kinds of measures that could be required. An organisation might, for example, be required to provide information about the design, configuration, operation or security of its IT systems, or details of any breaches or attempted breaches of the security of those systems. In practice, this could include information about firewall rules, anti-virus protection and network architecture. Potentially an even greater burden on an organisation would be if the Government were, on a 'preventative' basis, to mandate the implementation by that organisation of certain minimum data security standards.

A further power conferred on the Government is to authorise an organisation to direct a third party to provide the relevant information. For example, the Government might authorise an organisation to direct its hosting or cloud services provider to provide the required information.

Broad powers - but when can they be exercised?

Although the powers conferred on the Government are broad, the legislation does limit them in the sense that they can only be exercised where the Minister of Home Affairs is 'satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to the national security, essential services or defence of Singapore or foreign relations of Singapore.' Clearly, this is something of a subjective test and will do little to address concerns about the potential for abuse of power.

The concept of 'essential services' for these purposes is another aspect of the previous legislation that has been broadened. In addition to the elements which were already part of this definition (communications infrastructure, banking and finance, public utilities, transportation, key infrastructure and emergency services such as police or civil defence), 'essential services' now also includes aviation, shipping and health services.

Foreign relations of Singapore

The reference to 'foreign relations of Singapore' is also important. The Singapore Government has shown a willingness to cooperate with enforcement organisations in other parts of the world, which is perhaps an indication of the fact that communications infrastructure, and therefore the associated threat of cyber-attacks, is, by its nature, not limited to territorial boundaries. The Government has already announced that it is working with the European Cybercrime Centre (or 'EC3'), which itself was only launched on 14 January 2013. As such, the ability for the Singapore Government to exercise its powers under the new legislation in relation to 'a threat to the...defence of...foreign relations of Singapore' could be a useful one for the Government's cooperative efforts. But for Singapore organisations, it means that they could, for example, be required to disclose information in relation to an actual or potential cyber-attack beyond Singapore's borders - whether in Europe or elsewhere.

There are also implications for organisations outside of Singapore. Where an offence is committed under the legislation by 'any person in any place outside Singapore,' that person 'may be dealt with as if the offence had been committed within Singapore' where, for the offence in question, 'the accused was in Singapore at the material time or...the computer, program or data was in Singapore at the material time.' So for organisations that have any kind of presence in Singapore (whether a physical presence or a digital presence), or which do business with Singapore (for example, with Singapore-based cloud services, IT security or software providers), there is the potential to be pulled within the scope of the new law.

The first key concern that has been raised is about the prospect of organisations being required to disclose highly-sensitive commercial information such as network architecture and software source code.

Enforcing the new law

To further underline the concern with which the Singapore Government views this issue, the new law attaches criminal liability to a failure to comply. Unless there is a 'reasonable excuse,' there is the threat of a fine not exceeding $50,000 or, perhaps more concerning for senior management of organisations that could be affected, imprisonment for up to 10 years, or both. So organisations will certainly need to take any Government request under the legislation seriously.

Controversy

The new law is certainly not without controversy. Concerns are focused on four areas: confidentiality and data privacy, implications for third parties, potential for abuse and cost of compliance.

Confidentiality and privacy

The first key concern that has been raised is about the prospect of organisations being required to disclose highly-sensitive commercial information such as network architecture and software source code. This concern applies not only in relation to disclosure of information to the Government but also if a third party is required to provide information through the organisation that is the subject of the Government's request (for example - if a software vendor is required to disclose information to a telco that has received the request from the Government). There is also concern that the new law could potentially require the disclosure of personal data, whether it is relevant to the threat in question or not.

The Government sought to address these issues by including in the legislation various safeguards to protect the information obtained. The information obtained is to be used or disclosed only for the purpose of preventing, detecting or countering the threat. Otherwise, written permission would be required. Failure to comply with such obligations is itself an offence, carrying a maximum fine of $10,000 or imprisonment for up to 12 months, or both. The only exception to the obligation to disclose information is information that is subject to legal privilege. However, given the broad scope for which information could potentially be used ('preventing, detecting or countering'), these provisions may do little to address the confidentiality and privacy concerns.

Implications for third parties

What, meanwhile, about an organisation's legal or contractual obligations to third parties? The new law seeks to address this, too. It provides an organisation with immunity for acts done in good faith pursuant to Government directions. However, although the immunity from civil and criminal liability may be helpful in freeing up the organisation to take the required action, it is not likely to be good news for businesses with which they contract. This is perhaps less relevant for the issue of confidentiality, since standard contractual boilerplate often contains an exception to confidentiality obligations in the event of a governmental or regulatory intervention. However, what about a failure to perform to required service levels? For example, if a hosting provider is required by the Government to take certain actions to target a particular piece of malware and those actions result in service degradation or disruption constituting a failure by that provider to meet the service levels required in a customer contract,

the provider could claim immunity in legal proceedings against them by the customer. Without recourse to ordinary 'breach of contract' remedies, customers doing business with Singapore providers may seek to include alternative contractual mechanisms. This might, for example, include a right of termination if the provider becomes the subject of an action to which the new law relates. Alternatively, at the more extreme end of the scale, a potential customer with knowledge of the new law and its implications might think twice about selecting a Singapore-based provider.

Open to abuse?

Given the broad scope of powers and the broad right to exercise them, there has been concern in some quarters that the law is open to abuse. Christopher de Souza, MP, commented: 'It might be beneficial, it might be prudent, both for the public, as well as the government, to explain what threshold must be met, or what factors will play in the minds of the Ministry of Home Affairs, before the power to issue directions, is exercised.' However, the legislation is deliberately broad in scope, so it seems unlikely that the Government will provide any more detailed guidance. What the Government has offered is the prospect of pre-consultation. In its Second Reading Speech, the Government stated that, 'Before a certificate is issued by the Minister, CII [Critical Information Infrastructure] stakeholders will be consulted on the implications, where practicable.' The 'where practicable' would appear to be key here, since given the 'rapidly evolving nature and complexity of the threat' (to use the Government's description), it may well decide in many cases that pre-consultation is not appropriate. In Parliamentary debate, some MPs argued that a panel should be set up to review decisions after execution to safeguard against abuse. This was rejected by the Government, 'given the sensitivity and nature of the content' in question.

Cost of compliance

What, meanwhile, of the costs of complying with the new law? The Government's Second Reading Speech indicates that these costs are unlikely to be borne by the Government: 'It is...in the interests of a CII stakeholder to proactively invest in preventive cybersecurity measures. This is because a successful cyber attack could lead to significant financial loss and reputational damage for the CII stakeholder. Hence...CII stakeholders will generally be expected to bear the cost of these measures.' The prospect of bearing the cost of an action requested by the Government is potentially an onerous burden that organisations will need to bear in mind.

Conclusions: Singapore and beyond

Singapore has moved quickly in passing this legislation given that the amendments were only proposed just over two months ago. However, it seems likely that similar legislation will follow in a number of other jurisdictions. Brussels, for example, is reportedly finalising a bill that, amongst other things, would require the EU's Member States to set up local cyber-security agencies. Whether equivalent legislation in other jurisdictions will be as broad (both in terms of the scope of powers and the circumstances in which they can be exercised) as that which is now on the statute books in Singapore remains to be seen. But with the issue climbing legislative agendas around the world, and given the global nature of the perceived threat, it seems certain that the approach to cyber-security is going to require an integrated approach from organisations' legal, compliance and technical teams - both in Singapore and beyond.

Rob Bratby Managing Partner
Matt Pollins Associate
Olswang Asia
rob.bratby@olswang.com
matt.pollins@olswang.com

Self-regulation in German online behavioural advertising

The German Data Protection Council initiative

The German online behavioural advertisement ('OBA') sector recently launched a self-regulation initiative called 'German Data Protection Council for Online Advertising'[1] ('the Initiative'). It provides an insight into how the sector views its data protection obligations *vis-a-vis* web users in Germany.

At an EU level, Article 5(3) of the E-Privacy Directive[2] generally mandates opt-in consent to the types of cookies used for OBA; it is supplemented by Recital 66 of the Citizens' Rights Directive[3] which refers to users signifying consent via web-browser settings or settings in other applications. The Article 29 Working Party has asked the OBA sector to provide a mechanism for users to express prior opt-in consent to OBAs.

At a German level, the situation is less clear though, since Article 5(3) of the E-Privacy Directive has not yet been formally transposed into German law. While it is arguable that it is directly effective, no amendments have yet been agreed on to revise the relevant provisions of the Telemedia Act. The Initiative's fairly comprehensive rules provide an indication as to the German OBA sector's position here.

Codes of conduct

At its core, the Initiative is a (sub-) licensing body which controls how licensees may use a particular pictogram to inform website visitors if and how OBA data is collected. The underlying legal framework consists of two codes of conduct, rules on complaints handling, as well as the pictogram licence agreement itself. The licence agreement already contains several instructive provisions but it is the codes of conduct and, to a lesser extent, the rules on complaints handling, which regulate the collection and use of OBA data in detail.

Broadly speaking, advertisement networks and other entities (together, 'service providers') which place OBAs across domains on third party websites, are subject to the more onerous third party code of conduct. On the other hand, entities that serve OBAs exclusively on their own websites ('operators') fall under the first party code of conduct. Primarily, the codes of conduct oblige the licensees to give notice to web users about the OBAs that are shown. Such notice must cover, amongst other things:

- the identity and contact details of the operator or service provider, as applicable; and
- the types of data collected, the OBA purpose and the collected data's potential recipients.

Additionally, operators and service providers must enable web users to prevent the collection and use of their OBA data. For operators, this means either providing a technical solution or a clear description of how cookies can be blocked via web-browser settings. Service providers, on the other hand, must participate in a pan-European preferences management tool which allows individuals to opt-out of OBA based on the service provider or altogether.

Rules on complaints handling

These are relatively broad, principally enabling third parties (being individuals as well as data protection, consumer protection and governmental organisations) to try to influence a licensee's behaviour within the scope of the applicable code of conduct. Available sanctions range from formal reprimands to the licensee's exclusion from the Initiative. Financial sanctions do not currently form part of the rules.

Notice and consent under applicable law

German IT and data protection laws contain extensive duties, which specify the types of information web users need to be notified of. The informational duties in the codes of conduct therefore do not appear to add much. One exception is where OBA data does not constitute personal data (e.g. anonymous OBA data). It can be argued that the informational duties imposed by the codes are wider than in current German law.

As regards consent, the codes of conduct follow the implied consent/opt-out route rather than the opt-in route. This contrasts with the Article 29 Working Party's request for an explicit opt-in consent mechanism (see above) as well as the German state data protection authorities' preference[4]. Further, it appears to go against the trend in other EU Member States, which have already transposed Article 5(3) of the E-Privacy Directive into national law (e.g. the United Kingdom[5]).

The Initiative's position regarding consent is understandable considering the present uncertainty in German law in this area. Its pan-European preference management tool may also be seen as an attempt to meet, at least in part, the demands of Recital 66 of the Citizens' Rights Directive.

Conclusion

OBA service providers will view the Initiative as providing welcome guidance about an area of law that still requires clarification in Germany. Nonetheless, the question of what type of consent is required for OBA cookies under German law remains open. While it is being resolved, German web users should see benefits from the introduction of the Initiative's pan-European preference management tool as well as the enhanced informational duties placed on its members.

Johannes Jördens Associate
Hunton & Williams
JJordens@hunton.com

1. Available via http://www.ddow.de
2. Directive 2002/58/EC on Privacy and Electronic Communications, as amended.
3. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.
4. For e.g. Sections 5 para. 1, 13 para. 1 and 15 para. 1 of the Telemedia Act as well as Section 4 para. 3 of the Federal Data Protection Act.
5. Regulation 6, UK Privacy and Electronic Communications Regulations 2003.

The Dutch approach to the legality of hyperlinks

The debate in the Netherlands over the legality of hyperlinks with regard to whether such links infringe on the copyright of works on the internet has been reignited recently by a pair of court decisions, by the District Court of Amsterdam and the Appeal Court of Amsterdam respectively. Both courts ruled on cases where the hyperlinks were found to be unlawful, yet the legal grounds leading to such a verdict differed. Win Yan Lam, a Senior Associate at Hogan Lovells International LLP, examines these two decisions and the differing legal approaches that have emerged in relation to hyperlinks and copyright infringement.

Hyperlinks have been the subject of many disputes across the world, including in the Netherlands. Back in 2002, the Supreme Court of the Netherlands had a chance to consider this issue[1]. Some in the Dutch legal community viewed this decision by the Supreme Court as a threat to hyperlinks. The situation in that case was as follows: when a visitor of a website clicked on an image (a hyperlink), the text of a third party website would pop up in a frame of that third party website. The Supreme Court found that by clicking on the image, the third party text was retrieved and communicated to the visitor. The Supreme Court therefore concluded that this constituted a 'simple repetition' (in Dutch: *eenvoudige herhaling*) of the third party text. 'Simple repetition' is the criterion of infringement in the case of non-original writings that can enjoy protection under Dutch copyright law. In view of this, the aforesaid finding of the Supreme Court gave rise to an animated discussion on the legal status of hyperlinks in the Netherlands.

A decade later, two decisions - one by the District Court of Amsterdam and one by the Appeal Court of Amsterdam - have renewed the attention on the topic of hyperlinks. In both decisions, the conclusion was that the hyperlinks concerned are unlawful, but the legal grounds leading to this conclusion were not the same.

Hyperlinks may constitute copyright infringement

In September last year, the District Court of Amsterdam ruled that posting a hyperlink to copyright-protected content in the case at hand constituted copyright infringement[2]. In that case, the Dutch blog GeenStijl featured an article about leaked photos of a Dutch reality TV star. These photos were meant to be published in an upcoming edition of a magazine. The article on the website of GeenStijl contained a hyperlink which directed visitors to the leaked photos on a third party file sharing and storage website. When Sanoma, the publisher of the magazine, managed to have the photos removed from the file sharing website, the Dutch blog updated its article by posting a new hyperlink that directed the visitor to another third party website on which the photos were available. The publisher of the magazine succeeded in having the photos on that website removed too, but by then the photos had already spread across the internet and visitors of GeenStijl kept posting new hyperlinks to the photos by way of comment on the article.

The District Court of Amsterdam considered whether posting a hyperlink on the internet constitutes a communication to the public (in Dutch: *openbaarmaking*) within the meaning of Article 12 of the Dutch Copyright Act. If so, GeenStijl had infringed the copyright in the photos by posting the hyperlinks. The District Court held that the following circumstances are particularly relevant when assessing whether there is a communication to the public: (1) if there is an intervention, (2) as a result of which a (new) public is reached, and (3) if the intervention is aimed at making a profit. The District Court then used these three criteria to determine if the hyperlinks in the case at hand constituted a communication to the public.

First of all, the District Court considered that the photos at hand initially could not be easily found and accessed by the public. Only the small number of people who knew the exact URL of the two file sharing and storage websites could view the photos. Thus, by posting the hyperlinks, the blog had intervened to provide the public with access to the photos. Further, the article of GeenStijl read 'And now the link to photos you all have been waiting for.' In an update, the blog wrote: 'Not seen the photos yet? They are HERE.' In view of the foregoing, the District Court held that GeenStijl intervened in full knowledge of the consequences of its actions. Secondly, the District Court found that a new public was reached: 230,000 daily visitors of the blog. The only thing that these visitors had to do to get to the file with the photos was to click on the hyperlinks posted by GeenStijl. The third criterion was met, too: according to the District Court, GeenStijl had posted the hyperlinks with the intention of luring visitors to its website or to keep its current visitors. It also appeared that the article containing the hyperlinks was the blog's most viewed article of the year. All in all, the District Court concluded that by posting the

hyperlinks, the Dutch blog had communicated the photos to the public. Consequently, the blog had infringed the copyright in these photos.

The three criteria which the District Court applied are derived from case law of the European Court of Justice regarding the question of what constitutes a communication to the public[3]. That case law does not explicitly deal with the issue of hyperlinks, but apparently this did not dissuade the District Court from applying these criteria to hyperlinks. Clarity on this subject matter will be given by the European Court of Justice itself: in October last year, the Swedish Court of Appeal referred *inter alia* the following question to the European Court of Justice in the case between Svensson, et al. and Retreiver Sverige AB: 'If anyone other than the holder of copyright in a certain work supplies a clickable link to the work on his website, does that constitute communication to the public within the meaning of Article 3(1) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society?'[4]

Two Court decisions have renewed the attention for the topic of hyperlinks. In both decisions, the conclusion was that the hyperlinks concerned are unlawful, but the legal grounds leading to this conclusion were not the same.

Hyperlinks may also constitute an unlawful act

In the meantime, four months after the GeenStijl-decision, the Appeal Court of Amsterdam was to decide another case concerning hyperlinks[5]. In that case, a former maths teacher had posted hyperlinks on his website which directed the visitor to PDF copies of copyright-protected solutions to math problems on third party file storage websites. Contrary to the District Court, the Appeal Court did not use the three aforesaid criteria to assess the publisher's copyright infringement claim: the Appeal Court simply held that a hyperlink which merely 'shows the way' to a work does not constitute a communication to the public within the meaning of the Dutch Copyright Act.

Instead, the Appeal Court discussed, at much greater length, the question of whether the former teacher's posting of the hyperlinks constituted an unlawful act. The Court of Appeal considered that the hyperlinks made it possible or at least much easier for third parties to find the unlawfully published maths solutions. According to the Appeal Court, the availability of the maths solutions on the internet had a negative impact on the sales of the publisher. As a result of this, the publisher lost revenue. The Appeal Court therefore concluded that the former maths teacher had breached the standard of due care, which constitutes an unlawful act *vis-à-vis* the publisher. Probably in view of the GeenStijl-decision, the former teacher had also argued that his website was not aimed at making a profit: it was simply a hobby. The Appeal Court however rejected this defence, reasoning that the nature of his website does not alter the fact that he negatively affected the publisher's exploitation of the maths solutions.

Two possible approaches to hyperlinks in the Netherlands

The European Court of Justice is still to deliver its judgment in the Svensson/Retreiver Sverige AB case. It remains to be seen if that ruling will have any consequences for the way in which Dutch Courts deal with the issue of hyperlinks. For now, the two recent decisions discussed in the foregoing seem to give rights holders two possible approaches in the Netherlands when confronted with hyperlinks to copyright protected material.

In the first approach, copyright infringement can be argued using the three mentioned criteria: intervention, a (new) public and the aim of profit. In this approach, the focus is more on the party posting the hyperlink. Does this party post the hyperlink in full knowledge of the consequences of its action? Is it aiming to make a profit? In the second approach, the possible negative consequences of the hyperlink for the rights holder are the main consideration. In view of these negative consequences, the posting of the hyperlink may constitute a breach of the standard of due care which must be observed in society.

Win Yan Lam Senior Associate
Hogan Lovells International LLP
Amsterdam
winyan.lam@hoganlovells.com

1. The Supreme Court of the Netherlands 22 March 2002, NJ 2003/149 (El Cheapo).
2. District Court of Amsterdam 12 September 2012, MF 2012/23 (Sanoma/GeenStijl).
3. E.g. ECJ 7 December 2006, C-306/05 (SGAE/Rafael Hoteles).
4. Case C-466/12 (Svensson/Retreiver Sverige AB).
5. Appeal Court of Amsterdam 15 January 2013, LJN: BY8420 (Noordhoff).

Key e-commerce cases

Full reports in E-Commerce Law Reports Volume 12 Issue 6

Defamation

Trkulja v. Yahoo!/Google

Two juries in the Supreme Court of Victoria found that Google and Yahoo! defamed Mr Milorad Trkulja through results generated from their search engines. Mr Trkulja has been awarded damages totalling AU$425,000.

In 2004, Mr Trkulja was the victim of a shooting. Police did not believe this was linked to gangland violence. The shooting was featured on now-defunct website 'Melbourne Crime.' Mr Trkulja became aware that Yahoo! and Google search results provided links to this website, containing photographs of crime figures.

Mr Trkulja's solicitors wrote to Yahoo! and demanded they remove all copies of the article. Yahoo! declined and suggested that Mr Trkulja contact the 'Melbourne Crime' website. Mr Trkulja sued Yahoo! for defamation.

The jury found that the 'Melbourne Crime' article was defamatory of Mr Trkulja. Mr Trkulja suffered a loss of standing as a result of his apparent connection to criminals.

Google relied on the defence of 'innocent dissemination' and argued that it did not have the requisite intention to publish the images as its systems were fully automated.

Mr Trkulja argued that while Google's systems were automated, they were written by humans.

Justice Beach ultimately held that it was open to the jury to find that Google had intended to publish the images that its automated systems produced, as that was what the systems were designed to do upon a search request.

Norman Lucas Partner
Erin Hourigan Associate
Maddocks Lawyers
norman.lucas@maddocks.com.au
erin.hourigan@maddocks.com.au

Domain names

Walter v. Paris

On 29 September 2012, in the case of Jeffrey Walter v. Ville De Paris, a US court in Houston Texas, applying the US Anti-Cyber Squatting Consumer Protection Act, ordered the City of Paris to transfer the rights to the domain name parvi.org ('Domain Name') to a Californian individual as well as to pay $100,000 damages and $26,830 costs.

Paris had challenged Mr Walter's registration of the Domain Name, using ICANN's UDRP administrative proceedings, on the basis of the city's French trade mark PARVI. The Domain Name was transferred to Paris.

Mr Walter commenced legal proceedings against the city on the grounds of reverse domain name hijacking. Paris lost because the city refused to defend the proceedings. The key lesson for rights holders to draw from the case is that the US court had jurisdiction to hear the case in the first place.

By initiating the UDRP proceedings, Paris had been caught by ICANN rule 3(b)(xiii) that a Complainant 'will submit, with respect to any challenges to a decision in the administrative proceedings cancelling or transferring the domain name, to the jurisdiction of the courts,' at the location of 'either (a) the principal office of the Registrar or (b) the domain name holder's address (as shown on the Registrar's Whois database).' In the case of Mr Walter, both these locations where in the United States.

Any party that initiates UDRP proceedings should be aware of which court may have jurisdiction if an Administrative Panel's award is challenged.

Jonathan McDonald Associate
Akash Sachdeva Partner
Edwards Wildman Palmer
JMcDonald@edwardswildman.com
ASachdeva@edwardswildman.com

Broadcasting rights

Ofcom and Sky: the must offer remedy

An Ofcom decision requiring Sky to sell its Sky Sports 1 and 2 channels to its competitors at a regulated price was overturned in August 2012 giving Sky an important victory against its pay-TV rivals. Ofcom had been investigating the way that Premier League (PL) football was broadcast to UK consumers. Its main concerns were that Sky (as a wholesaler and retailer of PL football) could have had an interest in limiting the distribution of premium content, and that it could set its prices at a level as to make selling its Sky Sports channels uneconomical for its competitors.

In March 2010, Ofcom published a Decision imposing an obligation for Sky to sell its Sky Sports 1 and 2 channels to its platform competitors at a regulated price, determined by Ofcom. This would have provided a mechanism for other platform providers to gain access to Sky Sports 1 and 2 on fair and reasonable terms.

Sky appealed the Ofcom Decision on a number of grounds including the fact that Ofcom's evidence that it used to show that Sky did not constructively negotiate in good faith with other platforms for the provision of Sky Sports 1 and 2 was flawed. The Competition Appeal Tribunal (CAT), where the appeal was heard, ultimately accepted that Ofcom misinterpreted the evidence of the negotiations and as a result, Ofcom's conclusions were inconsistent with the evidence. As such, the CAT decided for this, and other reasons, that Ofcom's Decision should be overturned. At the time of writing, it is rumoured, that Sky's competitor BT may appeal the CAT decision.

Daniel Geey Associate
Field Fisher Waterhouse LLP
Daniel.Geey@ffw.com