e-commercelawreports

THE PRACTITIONERS' GUIDE TO E-COMMERCE CASES
VOLUME 12 ISSUE 04 WWW.E-COMLAW.COM
[2012] ECLR 1- 24

VOLUME 12 ISSUE 04 [2012] ECLR 1-24

EDITORIAL

Combating online piracy: an ongoing battle

Online piracy and how to combat the illegal downloading of music, movies and television shows, is the bane of the digital age. Net pirates have been roaming the online space for years and yet an efficient and adequate solution to the problem has yet to be found.

In June of this year, four music record companies: EMI Records (Ireland) Ltd, Sony Music Entertainment Ireland Ltd, Universal Music Ireland Ltd and Warner Music Ireland Ltd, won a court order in Ireland to overturn a ban on an anti-piracy policy operated by Eircom, Ireland's largest internet service provider (ISP). The court order reversed an enforcement notice issued by The Office of the Data Protection Commissioner in Ireland (ODPC), issued in December 2011, which banned Eircom from operating its 'three strikes' system, to prevent illegal music downloading.

Eircom's 'three strikes' system, which was agreed in collaboration with EMI, Sony, Universal and Warner, and approved by the Irish Government, warns customers suspected of illegal file-sharing that they risk being cut off from the internet. After three copyright infringements, customers lose access to the internet for a week, after four they lose access completely. The music companies challenged the Commissioner's enforcement notice, which sought to ban Eircom's 'three strikes' policy on privacy and data protection grounds, due to concerns surrounding Eircom's use of IP addresses to identify alleged infringers and following a complaint by a subscriber wrongly notified of a copyright infringement. The ODPC launched its investigation after Eircom sent its first round of warning letters to 300 customers wrongly accused of illegal file-sharing. A fault Eircom attributed to a software failure.

The Data Protection Commissioner's notice stated that Eircom was in breach of data protection law because of its monitoring of traffic data, which was not deleted after the monitoring process, and because of the manner in which it processed personal data, which was both incompatible with the purpose in which it was obtained and without the informed consent of subscribers. Eircom was then given 60 days to cease all processing and destroy any such personal data.

Ireland's Commercial Court however ruled that the ODPC had failed to give reasons in the notice as to why it had been issued, and that the apparent reasons relied upon to serve the notice, "involved a misconstruction of the relevant law". As a result the Court did not assess the data protection issues surrounding Eircom's 'three strikes' policy, which was deemed legal and not in breach of data protection laws by Ireland's High Court in 2010. The Court's decision means that Eircom can continue its 'three strikes' policy and actively monitor, notify and block users involved in the illegal downloading of music.

Under plans drawn up by Ofcom, ISPs in the UK will soon be required to issue similar notices to customers suspected of copyright infringement. The UK's Digital Economy Act aims to, amongst other things, make it easier for rights holders to enforce their rights against infringers, but the regulation of the online space remains a delicate balancing act. Internet users' rights need to be protected, as do the rights of copyright holders', but just how to find this balance, whilst maintaining online freedoms, which defines the very nature of the internet itself, is extremely complex. It seems to be an issue rooted to the very heart of the internet itself.

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 John Archer
john.archer@e-comlaw.com
telephone +44 (0)20 7012 1388
Sales and Marketing Karl Nitzsche
karl.nitzsche@e-comlaw.com
telephone +44 (0)20 7012 1382
Design MadeInEarnest
www.madeinearnest.com
Print The Premier Print Group

E-Commerce Law Reports is published 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

Apple Inc. v. Samsung Electronics Co. Ltd.

United States District Court, Northern District of California

Apple's landslide victory over Samsung in a US District Court, saw Samsung found guilty of willful infringement and liable for damages in excess of $1 billion. But such a ruling does not mark the end of the so called smart phone 'patent wars'.

As the smart phone wars continue to rage across the world, the verdict in the Apple v. Samsung case is the latest battle to end, at least for now, in favour of Apple. Given Apple's victory, it is likely Apple will continue to press its offensive across the globe, particularly in the US. Even though Apple has suffered some set backs, most recently in South Korea, the victory over Samsung in the Northern District of California will spur on additional lawsuits, both in the US and other countries. Until Google (perhaps through Motorola) or one of the Android handset makers, such as Samsung or HTC, achieves a victory over Apple, the smart phone wars are not likely to slow anytime soon.

The key aspects of the verdict included the numerous products of Samsung (over twenty in all) that infringed several Apple patents, several findings of willful infringement, a damage verdict in excess of $1 billion and a finding by the jury that Apple did not infringe any of the Samsung patents. Each of these items is significant on its own and when combined show just how significant a win this was for Apple - a win in which Apple essentially swept the board in everything but the amount of the damages and $1 billion in damages was hardly disappointing.

With the verdict in, there are still issues for the trial judge to decide, including whether to enhance the damages, award attorneys' fees in favour of Apple, and to determine whether a permanent injunction should issue. In addition, Samsung will seek to overturn the jury verdict arguing, among other things, that there is insufficient evidence to support the verdict, that the patents are invalid and that there were legal errors that should result in a new trial.

This next stage of the case will also prove difficult for Samsung. The difficulty arises not just from the size of the damage award of the jury verdict, but also from the sheer number of products found to infringe several Apple patents and the finding that Samsung willfully infringed several of these patents. The finding of willfulness permits the trial judge to award Apple its attorneys' fees and to enhance the damages up to three times the original amount of the verdict. Further, given the willfulness finding and some of the discovery ruling against Samsung before the trial began, it is likely that the trial judge will award at least some of Apple's attorneys fees. The district court may enhance the damage award as well, but this is less likely given the large size of the verdict that the jury already awarded.

In terms of the permanent injunction, given the preliminary injunction that issued before the trial began, it is likely that a permanent injunction will issue, at least on some of the products. Expect Samsung to ask for a sunset period, i.e. a period of time to design around the patents, before the injunction goes into effect. Samsung likely has already designed around (or attempted to design around) the Apple patents. There will likely be a number of motions filed with the district court on these issues and Apple, if successful in obtaining an injunction, will likely assert that many of the re-designed Samsung products still infringe the Apple patents.

Finally, expect Samsung, once the judgment is final, to appeal. It is not easy to overturn a jury verdict on appeal, but the Federal Circuit will review the verdict and the patent issues closely. There may be some room to challenge the damage award. Of course, given the number of products that were found to infringe and the size of the smart phone market, the jury award, at least at first glance, does not shock the conscience.

What will the impact of the jury verdict have on the other smart phone cases around the United States and the rest of the world? Given Apple's highly favourable verdict, it is not likely that Apple will stop the all out assault on Android and Android enabled devices. Even before the Samsung verdict, Apple has already had success against HTC in the US, at the International Trade Commission, and will likely continue to press its matters against HTC. With a much bigger verdict against Samsung, Apple will be even more encouraged to proceed with its assault not just against Samsung and HTC, but also against Motorola.

Ultimately, the smart phone war comes down to Apple v. Google. The many battles have so far focused on handset manufacturers, but the Android operating system lurks in the background. With Google's acquisition of Motorola, there is now a more direct line of litigation between Apple and Motorola. Motorola recently sued Apple in the US District for the District of Delaware and the International Trade Commission, which is further evidence that the smart phone wars are more likely close to their beginning than their end.

Ultimately, Apple will continue its all out assault until another company gains some leverage. That likely will not happen until one of these companies obtains a significant victory against Apple in court. As that is likely a long way off, expect the patent wars over smart phones to continue for some time.

Stan Gibson Partner
Jeffer, Mangels, Butler & Mitchell LLP
SGibson@jmbm.com

Australia's Advertising Standards Board and social media marketing

Companies may have to radically rethink their social media marketing in Australia as a result of decisions by the Advertising Standards Board. Decisions involving Victoria Bitter and Smirnoff confirm the position emerging from Australian courts, that brand owners must take responsibility for user posts on their social media pages.

Advertising Standards decisions - Victoria Beer

The Advertising Standards Board investigated a complaint that content on the Facebook page for Victoria Bitter (VB) beer breached the Australian Association of National Advertisers Code of Ethics. The Code sets out the principal advertising standards in Australia.

The Board determined that an advertiser's Facebook site is a marketing tool over which the advertiser has a reasonable degree of control and that the site is designed to promote the product. On that basis, the Board determined that the Code applies to a brand owner's Facebook page. Crucially, the Board further determined that the Code applies to all contents on the page - i.e. both the content posted by the brand owner and material or comments posted by users.

The Board held that the Code was breached because some user posts on the VB Facebook page were discriminatory toward women, degrading to homosexual people, used strong and obscene language and did not treat sex, sexuality and nudity with sensitivity to the relevant audience.

In its determination, the Board indicated that social media requires monitoring to ensure that offensive material is removed within a reasonable timeframe to ensure compliance with the Code.

The sanctions the Board can impose if an advertiser does not withdraw or modify advertising that breaches the Code essentially involve the Board publicising the matter, including contacting the media. In most cases where a Code breach has been found, the threat of adverse publicity has proved a sufficient sanction and the advertiser has removed the relevant material. In this case, the brand owner removed the material in question after being notified of the complaint, before the Board made its decision.

Smirnoff Vodka

Another recent determination by the Board involved the Australian official Facebook page for Smirnoff Vodka. Diageo, the brand owner, unsuccessfully argued that Facebook is a communications channel just like TV and radio and therefore it is not appropriate to consider all content as advertising material. The Board again expressed its view that the Code applies to content generated by advertisers as well as material posted by users - however in that case, none of the content was found to breach the Code.

In parallel to the above decisions under the AANA Code of Ethics, complaints about the Facebook pages for VB and Smirnoff were also examined under the Alcohol Beverages Advertising Code (ABAC). The ABAC Complaints Panel determined that the VB page breached the ABAC because certain user generated content, in conjunction with posts by the brand owner, encouraged excessive consumption of alcohol.

The Panel also found that the Smirnoff page breached the ABAC prohibition on using adults under the age of 25 in advertising. Smirnoff had posted photographs on the page of people who were of legal drinking age (18 or over) but who were under 25. The Panel considered that the Facebook page as a whole (including user-generated content) was an advertisement.

In considering these complaints the ABAC Complaints Panel found 'real difficulties' in applying the ABAC to the 'dynamic nature of social media' and that the ABAC was 'designed for a very different type of advertising'. It noted that a review of the ABAC scheme will be undertaken in the near future.

Since anyone can lodge a complaint under the AANA Code of Ethics or the ABAC, and the complainant's identity is generally not disclosed to the company complained about, companies could face complaints lodged by 'activists' or even by representatives of competitors, as well as members of the general public. In the case of the complaints to the Advertising Standards Board about the VB and Smirnoff pages, it has been reported that the complainants have publicly identified themselves. They are academics that lodged the complaints for 'academic purposes', curious to see what result the complaints might have under the complaints processes.

Court decision - Allergy Pathway case

The advertising standards' decisions are broadly consistent with the position emerging from Australian case law.

In the case of ACCC v. Allergy Pathway (No. 2) [2011] FCA 74 the Federal Court held a company and its sole director liable for contempt of court in relation to posts on the company's Twitter and Facebook pages.

The company and director had previously undertaken to the Court not to publish certain misleading representations about the company's services for treating allergies. After that undertaking was given, third parties posted testimonials on the company's Twitter and Facebook pages, endorsing the company's allergy treatments. The Court held that the third party posts led to contempt of court by the company and director because they knew that the testimonials had been posted but did not remove them. According to the Court:

...Allergy Pathway accepted responsibility for the publications

when it knew of the publications and decided not to remove them. Hence it became the publisher of the testimonials.

In reaching the above view the judge relied on defamation cases. Therefore the above logic could apply if a user posts defamatory material on a company's social media page and the company, knowing that the post has been made, does not remove it. Similar logic might apply in relation to material that infringes copyright or breaches a range of other laws.

How should brand owners moderate social media?

To avoid breaching advertising standards, companies need to moderate posts to their social media sites and may be held accountable if inappropriate material is not quickly removed. The same logic would apply to a company's website, if it is possible for users to post material to the site.

This could mean that companies have to devote significantly more resources to moderation, or else change their whole marketing approach to involve less interaction through social media and websites. Of course, more resources would mean more costs.

Moderation should be conducted by staff who are given clear guidance by the brand owner and who are capable of making sensible judgments. It is not simply a mechanical task - it could involve difficult judgments about which posts push the boundaries too far.

Brand owners can further limit their risk exposure by using some features offered by Facebook. For example, it is possible to restrict a Facebook page so that it can be viewed only by persons in a certain age demographic, e.g. over 18, or only by persons in particular countries.

Facebook also enables a page administrator to blacklist words so that comments containing those words are visible only to the commenter and their friends. In addition, particular users can be flagged so that their comments are only visible to themselves and their friends.

While these features limit the audience viewing potentially problematic posts, they do not completely eliminate the risks for the brand owner. The comments could still breach advertising standards or include, for example, defamatory material for which the brand owner might be held responsible.

How often must posts be removed?

To eliminate risk completely, moderation would have to be carried out 24 hours a day, every day of the year. Since this is not commercially viable for many brand owners, they will have to come to a view about how often they should moderate in order to contain risk.

In its response to the VB determination, the brand owner indicated that it now conducts twice daily monitoring of user comments including removal of inappropriate comments.

The Australian Consumer Law contains a broad prohibition on misleading or deceptive conduct. In recent weeks the Australian Competition and Consumer Commission (ACCC) has indicated that a company may breach this prohibition if it allows a misleading post by a consumer to remain too long on the company's Facebook page. For a large, well resourced company the ACCC's view is that misleading posts by users should be removed within 24 hours. A smaller company might be given more leeway but could still be held responsible if a misleading post - e.g. a post stating that the company's products have features or benefits that don't really exist - remains on the page for too long.

The clear message for brand owners is that they must actively moderate user posts on their websites and social media pages. It is to be hoped that they do not become too conservative in their judgments and remove all 'borderline' material so that these valuable opportunities for interaction with consumers become anodyne and unengaging.

David Smith Partner
Corrs Chambers Westgarth
david.smith@corrs.com.au

Content Services Ltd. v. Bundesarbeitskammer

European Court of Justice, 5 July 2012, C-49/11

A recent ruling by the European Court of Justice has provided useful insight into the meaning of Article 5 of Directive 97/7 on the protection of consumers in respect of distance contracts.

Background

Directive 97/7 on the protection of consumers in respect of distance contracts sets out the following legal obligations:

- There is certain information that a goods or services supplier must provide to a consumer prior to the conclusion of any 'distance contract' (e.g. a contract concluded online or by telephone), which includes:
  (i) the main characteristics of the goods or services to be provided to the consumer under the contract;
  (ii) the price (including taxes) of those goods or services;
  (iii) the delivery costs, if any;
  (iv) the arrangements for payment, delivery or performance;
  (v) the identity and contact details of the supplier; and
  (vi) the existence of the Right of Withdrawal (see below);
  the 'Information' (Article 4).
- The consumer must receive written confirmation of the Information in writing or via another durable medium available and accessible to the consumer in good time during the performance of the contract and, at the latest, at the time of delivery for goods, unless the Information has already been given to the consumer prior to the conclusion of the contract in writing or via another durable medium available and accessible to the consumer (Article 5).
- The consumer has the right to withdraw from the contract within the seven working days following either the date following the day of receipt of the goods by the consumer or the date of the conclusion of the contract for the provision of services, or, where the Information is not provided, three months from the relevant date (the 'Right of Withdrawal'). The consumer may not exercise the Right of Withdrawal in respect of the provision of services if performance of those services has already begun with the consumer's agreement before the end of the seven working day cooling-off period (Article 6).

The case

Content Services Ltd (CS) is an English-based company which operates a website on which it offers software for download. In order to download software from the website (sometimes for a fee), users have to fill in a registration form and, when they submit their order, users have to tick a box on the website to show that they have accepted CS's terms and conditions and that the user waives the Right of Withdrawal in respect of the software. Without ticking that box, users are unable to proceed with their order.

CS did not show the Information directly to users and, instead, a hyperlink was provided to users to access the Information via that hyperlink.

Following the submission of an order, CS sent an email to the consumer which contained a hyperlink together with a username and password. The consumer was able to access the Information by clicking on that hyperlink. The consumer then received an invoice for access to the content on the CS website, and the invoices set out again that the consumer had waived the Right of Withdrawal.

Why the action was brought

CS's website was accessible to consumers in Austria. The *Bundesarbeitskammer*, a consumer protection body in Austria, challenged CS's practices on the basis that those practices infringed various laws at both domestic and European Union level. Initial proceedings were heard by the *Handelsgericht Wien*, the commercial court in Vienna, and the court ruled against CS. CS then appealed to the *Oberlandesgericht Wien*, the regional high court in Vienna, which considered that, as the Information was available to a consumer only via a hyperlink, the Information was not available on a permanent and lasting basis. In order to reach the final ruling, the *Oberlandesgericht Wien* referred a question to the European Court of Justice (ECJ).

The question

That question was whether the provision to a consumer of a hyperlink to a website containing the Information, where the Information was not accessible via any other medium, was sufficient to meet the requirements of Article 5 of Directive 97/7.

The ECJ's ruling

Is the information 'given' to or 'received by' the consumer?

The ECJ did not consider that Article 5 set out the meaning of 'receive' and 'given' in the context of a consumer receiving or being given the Information, and so considered the plain meaning of those words in everyday use together with the context and purpose of their use in Article 5.

The ECJ decided that 'receive' and 'given' were two parts of the same transaction, one from the consumer's perspective and one from the supplier's perspective; in any event, it meant that the consumer, the receiver of the Information, did not have to take any particular action in order to receive it. By providing a hyperlink to the Information, CS was expecting the consumer to take a specific action in order to view that Information, being to click on the hyperlink.

The ECJ said that the context of the use of 'receive' and 'given' in Article 5 is to ensure that a consumer receives the Information for proper performance of the

contract and can make use of the Right to Withdraw and other consumer rights. Article 5 also used those words rather than a more neutral form, such as 'provide', which indicated that the consumer should need to exercise only passive conduct to come into possession of the Information. The preamble to Directive 97/7 sets out that the purpose of the Directive is to protect the consumer and make sure that, just because a contract is concluded at a distance, a consumer does not receive any less information than they would receive if the contract was not concluded at a distance.

Is a hyperlink a durable medium?

The ECJ noted that Article 5 sets out an option between 'writing' and 'another durable medium' for the consumer to access the Information, and, therefore, the 'durable medium' must ensure that the consumer is in possession of the information to enable the exercise of rights where necessary.

For the purposes of Article 5 of Directive 97/7, there is no specification of the meaning of 'durable medium' for the giving to the consumer of the Information. Therefore, the ECJ considered the meaning given to 'durable medium' in European Union Directives 2002/65/EC, 2002/92/EC, 2008/48/EC and 2011/83/EU. That meaning, in summary, is 'any instrument which enables the consumer to store information addressed personally to him in a way accessible for future reference for a period of time adequate for the purposes of the information and which allows the unchanged reproduction of the information stored'.

The ECJ considered that, for a medium to be considered durable, the supplier must address the Information to the consumer personally, ensure that the content of the Information is not altered, that the Information is accessible for an adequate period and that consumers have the opportunity to reproduce the Information unchanged.

The ECJ decided that CS's website did not allow a consumer to store the Information once it had been accessed in a way that it was personally addressed to that consumer, and accessible to that consumer so that it could be reproduced unchanged for an adequate period of time. Whilst some websites do allow for information to be stored, accessed and reproduced unchanged for an adequate period of time (referred to by CS and the ECJ as 'sophisticated websites'), CS's website did not allow for this, so the ECJ did not need to rule as to whether or not a 'sophisticated website' is a 'durable medium'.

Conclusion

The ECJ therefore ruled that providing the Information to be accessed via a hyperlink to CS's website was not sufficient to fulfil the requirements of Article 5 of Directive 97/7. The Information was neither 'given' nor 'received' by the consumer, as the hyperlink required more than passive action by the consumer to possess the Information, and the website was not a 'durable medium' that allowed, if the Information was posted on it, a consumer the opportunity to reproduce the Information unchanged for an adequate period of time.

The decision has now gone back to the *Oberlandesgericht Wien* for final ruling.

Simon Weinberg Solicitor
Matthew Arnold & Baldwin LLP
Simon.Weinberg@mablaw.com

Legal developments in commercial on-line banking

The state of on-line banking law in the United States has been clarified by two cases that have set legal precedent: the Bench Trial Opinion in Experi-Metal Inc. v. Comerica Bank, Case No. 2:09-cv-14890, and Patco Construction v. Peoples United Bank, 684 F.3d 197 (1st Cir. 2012), decision by the First Circuit Court of Appeals.

In Patco Construction v. Peoples United Bank, a lawsuit arising after a cyber account-take-over of a commercial customer's bank account, the First Circuit Court of Appeals ruled that a financial institution's electronic banking contract did not employ a commercially reasonable security procedure. The state of on-line banking law in the US is examined.

Businesses are increasingly turning to on-line and mobile functionality for their banking needs, and banks and non-banks are rapidly moving to meet expectations. Understanding the legal rules of the road permits all participants to evaluate their investments and the risks in the migration to cyber banking. The normative legal playing field on which financial institutions and their commercial customers interact is set forth in the United States primarily by the Uniform Commercial Code[1] (UCC). The UCC's rules governing electronic funds transfers are found in Chapter 4A[2]. One of the most important areas of commercial interaction relates to the parties' authentication of the electronic instructions communicated. The ultimate inquiry is whether the payment order received from one party, which is to be acted upon by the other, actually originates from a customer, and not an imposter. On this issue the UCC's 4A-202, primarily, supplies the operative authentication guidelines.

Nowhere are the legal e-commerce issues more important, and in more flux, than in situations where a cyber imposter successfully infiltrates a commercial customer's computer assets in order to initiate fraudulent transactions. This type of fraud is commonly called an account-take-over attack. It is in the context of account-take-over attacks that important electronic banking law is now being made.

Practitioners in the field tend to recognise two cases as the most important legal precedent - the Bench Trial Opinion in Experi-Metal, Inc. v. Comerica Bank, and the Patco Construction Company, Inc. v. Peoples United Bank, by the First Circuit Court of Appeals. Taken together, both Experi-Metal and Patco provide a survey of the salient issues most often implicated by the rules of the legal road found in the UCC's 4A-202's electronic authentication requirements.

Experi-Metal

On 22 January 2009, hackers initiated wire transfers from Experi-Metal's commercial bank account at Comerica Bank. The attack originated via a phishing email directed to one of the business' co-Administrators designated under the on-line banking product. The email directed the recipient to a fraudulent website, which accurately spoofed the Bank's real webpage. When Experi-Metal's Controller clicked on the malicious link, at 7:35 a.m., he unknowingly compromised his secure authenticating information, which in part was held on a secure physical token device. The criminals immediately opened an on-line transaction session, and kept it open until 2:02 p.m. In that time ninety-three fraudulent payment orders, including wire transfers, were initiated. The criminals also transfered balances from other Experi-Metal bank accounts, and even the business' President's own personal account, to the business's cash-management account. By 11:30 a.m., the Bank learned from another financial institution of suspicious activity in the Experi-Metal account, and at approx. 12:05 notified their customer. By 12:30 most account activity and all outgoing wire activity had been halted. In total, a little over $1.9M in fraudulent wire transfers had been initiated. But the quick work of the Bank, after reversing entries and other recoveries, the account's principal loss stood at approx. $560,000.

Experi-Metal brought suit in the State Courts of Michigan, which was removed on Comerica's motion to the federal court system. The first adjudication of the District Court in Michigan was to hear Comerica's motion for summary judgment, which the Court denied. But in its ruling, the Court importantly held that Michigan's statutory UCC, particularly 4A-202(2), provided the controlling law. Further, it found (a) that the person who committed the fraud had obtained Experi-Metal's confidential information from a company authorised user of the on-line banking product, and (b) that the parties' contract employed 'a commercially reasonable method of providing security against unauthorised payment orders.' This latter finding was in part based upon the contract's express language. Thus the Court ordered a bench trial for January 2011, to consider two remaining 4A-202 issues: (1) Whether the impersonated employee was authorised to initiate electronic wire-transfer orders and whether Comerica complied with the contractual security procedures during the loss event; and (2) Whether Comerica acted in 'good faith' when it accepted the subject payment orders.

In its Bench Opinion, dated 13 June 2011, the District Court found that the Experi-Metal employee, impersonated by the fraudster, was authorised to initiate the payment orders leading to the wire transfers. The Court also found that the Bank, in accepting the fraudulent instructions, complied with the written

contract. In short, the hackers, after gaining dominion over the 'right' authorised user's credentials, followed protocol in creating the fraudulent wires.

The Court turned to its second issue, the question of Comerica's 'good faith' in accepting the orders. As written into Chapter 4A of the UCC, on-line direction will not be effective as a customer unless the bank 'proves' it accepted the payment order in good faith. UCC 4A-202(b)(ii). 'Good faith,' as defined in §1-201(20) of the UCC, has both subjective ('honesty in fact') and objective ('observance of reasonable commercial standards of fair dealing') features. After hearing the evidence, the District Court ruled Comerica met its burden of proof under the subjective criteria, but not upon the objective prong. 'Comerica was required to present evidence from which this Court could determine what the reasonable commercial standards of fair dealing are for a bank responding to a phishing incident such as the one at issue and thus whether Comerica acted in observance of those standards.'

The court ruled that the Bank's expert witness was not qualified to instruct on cyber wire transfer activity and phishing issues, because the expert was considered to hold no actual internet banking experience. It also appears that the Court was influenced by the specific facts of the event. Of particular note was the volume and frequency of the payment orders in comparison to traditional account activity, a $5 million overdraft created by book transfers in what typically was a zero balance account, the customer's limited prior wire activity, and then to virginal beneficiaries and RDFI's, and the Bank's knowledge of similar phishing attacks having been attempted in the past. The Court ruled the Bank had not met its burden of proof, and under this section of the UCC all 'ties' go to the account customer.

Patco Construction

Sometime in May 2009, Patco permitted its network to be infected by Zeus/Zebot derived malware. As a consequence, a hacker was able to initiate six fraudulent ACH transfers over six days, between 7 to 14 May 2009, from its account at Ocean Bank, a division of Peoples United Bank. Despite being a regular user of the Bank's e-banking functionality, Patco did not dispute any transaction until 14 May, when arguably the Bank's own mailed notice (respecting returned items from the first day's ACH batch) was received by Patco. In total, over $588,000 in ACH transactions had been authorised by the fraudster.

In the eyes of the First Circuit it was important context, during Patco's six years as an on-line banking customer, that it had used its on-line account only for payroll purposes, and then only on Fridays, that its payment orders always originated from a single static IP address, and that its largest prior ACH batch had been approx. $36,000 (compared to the fraudulent batches in amounts of $56,000 to $133,000). Further, the Court perceived the Bank had information the fraudulent payment orders were originating from foreign devices, originating from terminal(s) that did not contain a Bank imbedded 'device cookie,' and that each order had high 'risk scores' (563-790), when in the past the highest risk score for a legitimate transaction had been 214.

The parties' contractual security procedures for the authentication of cyber payment orders included: (a) User ID's and passwords; (b) Device authentication, i.e. a cookie placed onto the customer's computer to identify machines; (c) Risk profiling to determine if a transaction differed from the user's normal usage; (d) Challenge questions employed if the transaction was deemed high risk; and (e) A dollar amount rule, which in this case was set at a threshold amount of $1. The Court commented on the security measures the Bank elected not to use, including out-of-band authentication, user-selected picture, physical tokens, and monitoring of risk-scoring reports.

Article 4A generally places the risk of loss with the Bank whenever an unauthorised funds transfer occurs. The First Circuit noted there are two ways this risk of loss may be shifted away from the Bank. One, the Bank may show that the payment order is an authorised order of the customer, either in fact or under the law of agency, under UCC 4A-202(a), which could not be proven here. The second way in which the risk of loss may be transferred is via the parties' contract. This must be accomplished in accordance with the rules set forth in UCC 4A-202(b) & (c), including its requirement that the contract provide a commercially reasonable method to authenticate payment orders received. Importantly, this is a question of law for the Judge, not a jury, to decide. There are two approaches acceptable for determining whether a designated security procedure meets that UCC standard. The first is by study of the selected protocol to determine if it meets the wishes of the customers, any circumstances of the customer known to the Bank (such as historic usage), alternative security procedures offered/rejected by the customer, and analysis of what similarly situated banks are employing. The second approach relies upon a UCC created presumption of

reasonableness, if the customer selected the protocol used, provided that the customer first had been offered (and rejected) an alternative security procedure that was commercially reasonable. Once the financial institution has shown both commercial reasonableness of the contract's security procedure and that it accepted the payment order 'in good faith and in compliance with the security procedure,' the risk of loss passes to the account customer.

The First Circuit examined the Bank's system and found it provided a reasonable method for authenticating on-line transactions. Patco argued that the Bank's decision to lower the security protocol's 'dollar threshold amount' to the value of $1 was unreasonable. The Bank's position was that this system wide low dollar threshold was designed to combat low dollar fraud. However, Patco argued that such a low threshold increased the times users were obligated to enter answers to the challenge questions, increasing the risk that a hacker with key logging malware learn the answers. In the Court's view, the Bank's approach 'did substantially increase the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and regularly high dollar transfers.'

Then, when the Bank had warning that such fraud was likely occurring, the Court concluded the Bank 'neither monitored that transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable.' The Court concluded that the Bank did not effectively use the information created through its security procedures, as the principal consequence of a flagged transaction was the imposition of challenge questions. The Court found that challenge questions alone are not adequate, to the exclusion of further controls, for the purposes of legally sufficient security procedure. The First Circuit's opinion did not reference the Federal Financial Institutions Examination Council's ('FFIEC') most recent Supplement as a source for its technical conclusions on this point, nor would that Supplement have been relevant to the Patco events, which occurred before publication; it is worth observing that the Court's conclusion is generally in accord with the FFIEC's Supplement's direction.

The Court found fault with the Bank's failure to implement additional security procedures as they became available in the marketplace. 'Ocean Bank introduced no additional security measures in tandem with its decision to lower the dollar amount rule, despite the fact that such security measures were not uncommon in the industry and relatively easy to implement.' In short, whether because the Bank unilaterally changed one component of the contract's security procedures or because in the Court's view the Bank is the more sophisticated party, the Court appears to suggest that an implied duty of technological evolution exists that may become a care taking duty imposed upon financial institutions respecting even their existing electronic banking contracts.

'The collective failures, taken as a whole, rendered Ocean Bank's security procedures commercially unreasonable,' the Court held in conclusion. For this reason, the First Circuit Court of Appeals reversed the lower Court's award of summary judgment in favour of the Bank and remanded the case to the District Court for further proceedings.

The Circuit Court affirmed the District Court's decision to deny Patco's own cross-motion for summary judgment. Various issues of fact prevented the imposition of summary judgment in favour of the account owner. 'The District Court did not reach, and the parties have not briefed, the question of what, if any, obligations or responsibilities Article 4A imposes on a commercial customer even where a bank's security system is commercially unreasonable.' The First Circuit also dismissed Patco's separate negligence cause of action, as being inconsistent with the duties and the liability limits set forth in Article 4A of the UCC. This precedent, which is in complete accord with Experi-Metal, is a silver-lining decisively concluding that common law negligence has no role to play in modern electronic banking authentication lawsuits.

Thus the Patco case has been remanded back to the lower court for further proceedings, with these final words of wisdom from the Circuit Court, 'On remand, the parties may wish to consider whether it would be wiser to invest their resources in resolving this matter by agreement.'

William T. Repasky Co-Chair Financial Services Litigation
Frost Brown Todd LLC
brepasky@fbtlaw.com

1. The Uniform Commercial Code has been adopted in principal in all 50 states in America, and this includes §4A-202, which is the focus of this article.
2. If any part of the funds transfer is covered by the Electronic Funds Transfer Act, 15 U.S.C. 1693 et seq., the entire transaction is excluded from Article 4A. See also 4A-108, which is presently being re-evaluated by sundry States. But generally, Chapter 4A is limited to commercial electronic banking.

Pirated android app websites targeted by the US Department of Justice

The US Department of Justice's recent seizure of three website domains has heralded the latest development in the digital piracy saga. Applanet.net, appbucket.net and snappzmarket.com are all alleged to have distributed Android apps for free and in breach of copyright.

The three sites were by no means insubstantial; the FBI announced that they had downloaded 'thousands of copies' of the apps as part of the investigation. Applanet alone still boasts 88,000 fans on Facebook and 21,000 followers on Twitter. Each website now displays a FBI banner, warning first time copyright offenders that they can face up to five years in jail and a $250,000 fine.

The seizure involved international law enforcement authorities, including those in France and Holland, as well as nine search warrants across six different US states. A statement released by the DOJ announced that 'cracking down on piracy of copyrighted works - including popular apps - is a top priority of the Criminal Division. Software apps have become an increasingly essential part of our nation's economy and creative culture, and the Criminal Division is committed to working with our law enforcement partners to protect the creators of these apps and other forms of intellectual property from those who seek to steal it.'

Although the DOJ has said that this is the first time website domains involving smart phone apps have been seized, recent months have seen law enforcement authorities take action against file sharing sites. Last month the operator of Surfthechannel, Anton Vickerman, was jailed for four years for two counts of 'conspiracy to defraud' by a court in Gateshead. The site, which linked to pirated films and other content, had estimated annual profits of £300,000. The Ukrainian based bit-torrent site Demonoid was taken down to a backlash from the Anonymous hacking community. Before its shutdown, the site had been ranked within the top 300 most visited sites in US.

In January US authorities seized file storage site Megaupload with prosecutors alleging that its pirated movies and other content has cost copyright holders $500m. The site's founder, Kim Dotcom, faces a jail sentence of up to 20 years if extradited from New Zealand and convicted in the US. UK ISPs have also acted to block file sharing site Pirate Bay following a High Court ruling in February. The site is said to have generated up to $3m in advertising last October whilst its co-founder, Gottfrid Svartholm Warg, has just been deported from Cambodia in order to serve a one year jail sentence in Sweden.

Such positive action against pirates is welcomed by copyright owners but has also been described as 'a massive game of whack-a-mole'. Countless alternative sites exist and it remains very easy to recreate the sites at another web address. The cost and effort involved in policing piracy by these methods means enforcing the block across the internet is almost impossible. Google recently revealed that it receives more than a million requests a month from copyright owners seeking to remove their content from its search results.

Last week Google announced that over half a billion devices are now using its Android operating system. However, application developers remain wary of Android, with sites like Applanet demonstrating that its business method does nothing to halt piracy. Unlike Apple's iTunes, apps for Android can be downloaded and installed without using its centrally controlled marketplace, Google Play.

In July developer Madfinger Games released its game 'Dead Trigger' onto Android for $0.99. Within a month the company's Facebook page stated 'even for one buck, the piracy rate is soooo giant, that we finally decided to provide Dead Trigger for free.' Madfinger are not alone. The developers of Football Manager, Sports Interactive, reported in April that the game's Android piracy rate was 9:1, or one sale for every nine pirate downloads. Korean developer Com2uS has cited a 98% piracy rate on its Android games whilst US developer, Appy Entertainment, has reported a piracy rate of 70:1 for its FaceFighter Gold game on Android against a 3:1 rate on iOS.

Crucially, despite the huge growth in Android uptake, neither Sports Interactive nor Appy Entertainment have released a game on the system since these experiences. To developers pirated copies don't just represent lost sales, they attribute to increased server, support and security costs. However, consumers remain attracted to free downloads and Android's self-sign certification as rights holder, which enables easy misrepresentation of ownership. Those downloading pirated apps should beware of possible malware and the risk of falling foul of law enforcement agencies.

Sports Interactive have called on Google to introduce an online store 'that essentially acts like an app-only iTunes' in order to regain control of the marketplace, but this is unlikely to suit Android's open access model. Google have announced that app encryption, whereby paid apps receive a device specific key before installation, will be introduced as part of its Android 4.1 (Jelly Bean) platform to be released later this year. Google and the developers will both hope that the encryption and continued legal action stave off the pirates and allow more apps to be uploaded onto the otherwise impressive Android system.

Natalie Elsborg Senior Associate
Oliver Price Trainee
Charles Russell LLP
Natalie.Elsborg@charlesrussell.co.uk

SAS v. World Programming and Oracle America v. Google

Judges in EU and US courts respectively have applied the 'idea, expression dichotomy' tool to reach an outcome in cases involving software copyright, reaching verdicts that place concepts such as ideas and methods of operation outside the realm of copyright protection.

In May, two decisions were given which suggest that EU and US copyright laws may be converging in their approach to determining the scope of protection afforded to software by means of copyright. Both decisions applied the 'idea, expression dichotomy', a doctrinal tool used in some common law jurisdictions to balance the public interest in incentivising investment in creativity with the public interest in maintaining free access to information at a level that facilitates innovation, economic progress and free discourse. This case review looks at these two decisions in so far as they consider the application of this doctrine to questions of software copyright.

The disputed technologies

In Case C-406/10 SAS Institute Inc. v. World Programming Ltd (SAS v. WPL), the Court of Justice of the European Union (CJEU) considered questions pertaining to a claim made by SAS Institute that a software system developed by World Programming infringed copyright subsisting in its software products.

SAS Institute is a business analytics software company. It provides an integrated set of software products and services to meet data management, advanced analytics and reporting requirements. One of SAS Institute's software products, Base SAS, is a platform that enables developers to write and run software applications written in the programming language known as 'SAS Language.'

World Programming designed a competing platform on which applications developed on Base SAS and in the SAS Language could operate. In designing its system, World Programming studied and observed the behaviour of SAS' software, reviewed its manuals and operated a 'Learning Edition' of Base SAS, with the intention of creating software emulating the functionality of SAS' software. There was no evidence to indicate that World Programming had access to the source code underlying any of SAS Institute's software products.

In Oracle America Inc v. Google Inc, US District Court Judge Hon William Alsup ruled on the 'copyrightability of certain replicated elements of the Java application programming interface.' The Java platform was first developed by Sun Microsystems, which was acquired by Oracle in 2010 and merged into Oracle America, the party to the proceedings. Similarly to Base SAS, the Java platform enables software developers to write and run applications. Applications written using the Java platform are written in the Java programming language and can operate on different types of hardware.

The Java application programming interface (API) can be described as a component of the Java software platform (although software developers generally tend not to conceptualise it in these terms). In lay terms, application programming interfaces enable software components to communicate with one another and hardware components to communicate with software components. In the words of Judge Alsup, an API acts as "a set of pre-written programs [designed] to carry out various commands, such as printing something on the screen or retrieving the cosine of an angle".

At the time of the dispute, the Java API had 166 packages containing six hundred pre-written programs that carried out over six thousand subroutines. Google, in 2005, in following a strategy to expand into the mobile device market, developed the Android software platform, which it wrote in the Java programming language. The Android platform has an API of its own, which at the time of the dispute was divided into 168 packages, 37 of which enabled the same functionality as Java API packages. The 37 packages in question had been given the same names as corresponding Java API packages and followed the organisational structure for Java API packages. The actual code used by Google to implement the API packages, however, was not in dispute.

Ideas and expression

In SAS v. WPL, the CJEU continued its trend of identifying provisions of international agreements to which it suggests its judgments must conform, noting that 'copyright protection extends to expression and not to ideas, procedures, methods of operation or mathematical concepts as such.' On this basis, the court reasoned that:

- affording copyright protection to software 'functionality' would make 'it possible to monopolise ideas, to the detriment of technological progress and industrial development';
- innovators should be left 'the desired latitude to create similar or even identical programs provided they refrain from copying'; and
- a distinction may be drawn between expressions which enable 'the reproduction of a computer program' and software elements 'by means of which users make use of the features of [a] program,' the latter falling outside the scope of copyright protection.

The CJEU did not however provide any guidance as to how to distinguish elements of source code that enable the reproduction of the computer program from those that enable the user to make

use of the features of a program.

Ideas and expression

In Oracle America v. Google, Judge Alsup considered in more practical terms the coding practices undertaken by software developers. He reasoned that a distinction may be drawn between a 'method specification' and 'method implementation'. Incorporating elements of a programming language necessary in order for a formulation of source code to achieve a functional result merely amounts to the reproduction of method specification. Method specification could never result in copyright infringement, as 'The method specification is the idea.'

For Judge Alsup, the analysis ought not to be about the level of creativity that goes into formulating a method specification. While he acknowledged that 'inventing a new method to deliver a new output can be creative, even inventive,' protection of such creativity or inventiveness must be determined solely in accordance with patent laws. Judge Alsup noted that a finding otherwise 'would bypass [the] entire patent scheme and claim ownership over any and all ways to carry out methods for 95 years [in accordance with US copyright laws].'

Formulation of source code beyond incorporating elements of a programming language essential to achieve a specified function, may amount to acts to which copyright protection attaches, as 'The method implementation is the expression.' The caveat was that in some circumstances it becomes difficult to distinguish between specification and implementation. In these circumstances, Judge Alsup, bound by governing case law, suggested that the 'merger doctrine' should be applied. 'When there is only one way to express an idea or function, then everyone is free to do so and no can monopolise that expression.' It was not without difficulty however that Judge Alsup applied the merger doctrine. He highlighted that particularly in its application to software, it means that '...non-efficient structures might be copyrightable while efficient structures may not be.'

Comment

The two cases highlight that accessibility to platform technology is a new battleground on which questions of investment in innovation and competitiveness of markets are being fought. Conscious of these underlying interests and the dangers of restricting access to information, both courts favoured a more expansive interpretation of the scope of subject matter that falls outside the scope of copyright protection than that allowed by courts in the past. While the decisions illustrate that the idea, expression dichotomy can be used as a lever to determine the extent to which elements of source code may be subject to copyright restriction, each decision highlights the difficulties inherent in following this interpretation.

As Judge Alsup identified, an analysis which begins by attempting to separate idea from expression and affords protection to what has been identified as expression except where there is only a limited number of ways of expressing an idea, encourages developers to invest efforts in developing inefficient workarounds to demonstrate that the methods they are following have been implemented differently from that pursued by others. Encouraging such behaviour is at odds with the fundamental purpose of copyright law to maximise the supply, quality and diversity of creative works having regard to the effects of such maximisation on the overall economy. As an unexpressed idea is not in need of protection, and given the efficiency dilemma, it appears that as an analytical framework, the idea, expression dichotomy is not an appropriate vehicle for reconciling the need for protection of creativity with the desire to allow greater access to and use of information for the purposes of facilitating innovation.

As noted in the CJEU's decision in SAS v. WPL, in addition to 'ideas', the international copyright agreements place 'procedures' and 'methods of operation' outside the scope of copyright protection. A more constructive analysis may be to identify the extent to which a particular expression of source code amounts to the formulation of a procedure or method of operation, rather than thinking in terms of what is idea and expression. If international norms are to be followed, procedures and methods of operation must be viewed as a means of carrying out an idea that are outside the scope of copyright protection.

What is certain is that protection of platform technologies will continue to be a matter of debate. Whether it is a social media platform, an investment platform, a mobile device's operating system or a software development platform, there is still a need for courts to engage in focused, empirically based analysis in order to provide greater certainty as to the extent to which copyright protection in software may be maintained, particularly in light of growing uncertainty as to the validity of such protection as an enabler of innovation.

Luke Scanlon Out-Law Lawyer
Pinsent Masons LLP
luke.scanlon@pinsentmasons.com

Nguyen v. Barnes & Noble

Case No. 8:12-cv-0812-JST (RNBx) (C.D. Cal. Aug. 28, 2012)

Companies in the e-commerce space take for granted the enforceability of terms of service contracts posted on websites, but as this recent order suggests some procedural guarantee may be required by courts in the United States.

Two cases, both written by the Seventh Circuit's Judge Frank Easterbrook, laid the groundwork with respect to clickwraps, browsewraps and rolling contracts: ProCD v. Zeidenberg, 51 F.3d 1447 (7th Cir. 1996) and Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997) cert. denied 522 U.S. 808 (1997). In ProCD, Judge Easterbrook considered whether terms of sale provided after a sales transaction of certain software could bind a purchaser. In that case, Zeidenberg, purchased ProCD's software in a retail store. However, the terms and conditions applicable to the software were not accessible to the defendant until he had completed his purchase, left the store, opened the box, and inserted the media into his computer. Zeidenberg subsequently created a website that offered the contents of the CD for a lower fee than ProCD, a clear violation of the software's terms of use. Zeidenberg argued that he was not bound by the terms of use because, during the late 1990s, standard practice was to put the terms of use for purchased software outside the box for the purchaser to consider prior to purchase. Without knowing the terms prior to his purchase, Zeidenberg argued, he should not be bound by them. Judge Easterbrook disagreed. He overturned the 'outside the box' standard, ruling that this practice was unrealistic and inefficient. The ruling in ProCD adjusted industry convention to allow terms of use to be introduced after the customer leaves, so long as the purchaser has a reasonable opportunity to return the software after being made aware of the terms.

A year later, Hill extended the ProCD standard in a case involving product sales over the phone. Judge Easterbrook held that a contract between a purchaser and seller does not form at the time of purchase because the purchaser has not, at that point, accepted the contract's terms. He introduced the notion that a contract can be created when the purchaser expressly indicates her acceptance-for example by declining to return the product within a specified time. The resulting doctrine meant that sellers can bind purchasers to terms of sale or use even after the transaction, even if the purchaser is unaware of the additional terms and the purchaser's acceptance of the terms is evidenced by simply not returning the item. And thus the 'terms later' or 'rolling' contract was born.

Contracts of adhesion are those that are offered on a 'take it or leave it' basis - if the buyer does not agree to the terms, he does not get the product or service. Rolling contracts are one variety of contracts of adhesion. With the internet's rise has come an increasing reliance on contracts of adhesion: for practical purposes, this approach streamlines website use and commercial transactions where standard contracts would be unwieldy. See 1-3 Corbin on Contracts § 3.37A ("... [T]he importance of enforcing these clauses for reasons of efficiency removes the last vestige of the fundamental concept of mutual assent. The old rule that one has a 'duty to read' such clauses and the failure to read them is no excuse to their enforceability is a snare and a delusion"). Typically, these agreements are entered into electronically and in one of two forms: clickwrap or browsewrap.

On one hand, some e-commerce sites employ clickwrap (or 'clickthrough') agreements, where the seller (and website host) makes the terms and conditions on which the seller is willing to deal immediately available to the customer, and offers the customer the chance to click some type of 'Accept' or 'I Agree' button. This 'click' is considered an affirmative indication of the customer's assent to be bound by the agreement's terms. Courts generally embrace clickwrap agreements, finding that when the user is presented with terms and clicks 'Accept,' is put on actual notice of both the terms' existence as well as constructive notice of the terms' substance. In the spirit of the ProCD decision, courts often hold that with a clickwrap license, a user's options are obvious and unambiguous: if he is willing to deal on the seller's terms, and he actively clicks 'Accept,' then he should be bound by those terms. In the alternative, if he does not wish to deal on those terms, he can click 'Reject' and refuse the transaction (or, theoretically, he could revise the seller's agreement and engage in some bargaining). See, e.g., Lozano v. AT&T Wireless, 216 F. Supp. 2d 1071 (C.D. Cal. 2002); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305 (Wash. 2000); Westendorf v. Gateway 2000, Inc., 2000 Del. Ch. LEXIS 54 (Del. Ch. Mar. 16, 2000), aff'd, 763 A.2d 92 (Del. 2000); Brower v. Gateway 2000, Inc., 246 A.D.2d 246 (N.Y. App. Div. 1998).

On the other hand, browsewrap agreements are more typically used as the format for website terms of use. Unlike clickwrap agreements, browsewrap agreements may bind users despite the lack of formal *indicia* of assent (e.g. by clicking 'Accept' or signing a contract). Browsewraps rely on the notion that browsing a website is sufficient evidence of a user's agreement to abide by the contractual terms of use, which are usually available in the form of a hyperlink located on a website's footer. Although many attorneys advising clients with websites have come to presume that browsewrap agreements are

enforceable, the precedent is far from consistent or determinative. One case that shakes the presumed reliance on enforceability is Specht v. Netscape Commc'ns Corp., 306 F.3d 17 (2d Cir. 2002). Sotomayor held that the browsewrap at issue was not legally binding: the plaintiff did not have sufficient notice, and therefore should not be bound to terms of a contract that they did not know existed. Most, if not all, courts adhere to some version of this notice requirement, although the lengths to which the party proposing the terms of use must go to give such notice differ widely across jurisdictions. Some courts require only minimal notice (e.g. a statement that terms of use exist somewhere on the site), while others have found browsewraps unenforceable when all that was required of the party to be bound was to simply scroll down the page to find the terms. Compare Affinity Internet, Inc., d/b/a SkyNetWeb v. Consolidated Credit Counseling Services, Inc., 920 So. 2d 1286 (Fla. Dist. Ct. App. 2006); Sw Airlines Co. v. BoardFirst, L.L.C., No. 3:06-CV-0891-B (N.D. Tex. Sept. 12, 2007); Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927 (E.D. Va. Sept. 15, 2010) with Burcham v. Expedia, Inc., 2009 WL 586512 (E.D. Mo. Mar. 6, 2009); Hubbert v. Dell Corp., 835 N.E.2d 113 (Ill. App. Ct. 2005).

Barnes & Noble's ill-fated tablet promotion

In the most recent case involving browsewrap enforceability, the plaintiff Nguyen's claims arose from a botched promotion made by the bookstore chain, Barnes & Noble, which offered discounted computer tablets - $101.95 for a 16GB HP TouchPad Tablet. Nguyen claimed that on 21 August 2011, he submitted an order in time to 'accept' the promotional 'offer' Barnes & Noble had made available, citing confirmation of his acceptance with an email correspondence he had received, confirming that his order had been received. The next day, Nguyen received an email from Barnes & Noble stating that the company was canceling his order because they had sold out. As a result, Nguyen alleged that he was 'forced to rely on substitute tablet technology, which he subsequently purchased . . . [at] considerable expense.'

Barnes & Noble's website Terms of Use-in the form of a browserwrap agreement-provided: 'By visiting any area on [barnesandnoble.com], creating an account, [or, among other things,] making a purchase via [the site] . . . a User is deemed to have accepted the Terms of Use.' In April 2012, Nguyen filed suit, alleging various consumer protection violations, including false advertising, unfair competition, and breach of contract, under both California and New York law. Barnes & Noble's moved to compel arbitration based on an arbitration clause embedded in the Terms of Use. The question before the court was whether the arbitration clause in the website's Terms of Use was enforceable in this situation.

The court ruled that the arbitration clause in the browserwrap agreement was not enforceable because the agreement itself was not enforceable. Following the reasoning in Sw. Airlines Co. v. Boardfirst, LLC, Judge Tucker argued that "the validity of a browsewrap license turns on whether a website user has actual or constructive knowledge of a site's terms and conditions." Like Sotomayor in Specht, Tucker ruled that the Terms of Use could not bind Nguyen because Barnes & Noble "did not position any notice even of the existence of its 'Terms of Use' in a location where website users would necessarily see it, and certainly did not give notice that those Terms of Use applied, except within the Terms of Use". Tucker distinguished Barnes & Noble's authorities one-by-one, arguing that not one of the cited cases dealt directly with the issue of whether the question of notice and assent to the terms sought to be imposed. Judge Tucker ultimately held that a reasonable person would not have known of the Terms of Use (and that Nguyen did not know of them), therefore Nguyen could not be bound by them.

Parting Thoughts

Nguyen is a wake-up call to corporations and attorneys who rely on the presumption that browsewrap terms of use will be enforced. Courts tend to draw a definitive line in cases where website users have actual or constructive notice of the existence and applicability of terms of use. Although the case law is still evolving, a conservative approach for e-commerce site administrators would be to use clickwrap agreements in lieu of browsewraps, as clicking 'Accept' is strong evidence that a party has affirmatively assented to be bound by applicable terms of use. Where a clickwrap is not feasible, e-commerce sites are well advised to make substantial efforts to make their terms of use conspicuous-first, by placing them in a prominent place and second, by explicitly drawing the user's attention to the terms at some point during a transaction. In circumstances like these, low-cost solutions can breed significant value in the long-term.

Timothy Denny Greene Associate
Debbie Rosenbaum Associate
Morrison & Foerster LLP
tgreene@mofo.com
drosenbaum@mofo.com

Samsung Electronics (UK) Limited v. Apple Inc.

[2012] EWHC 1882 (Pat) (9 July 2012)

Samsung sought a declaration that three of its Galaxy tablet computers did not infringe a Community Registered Design belonging to Apple. The High Court Judgement deemed there to be no infringement in the UK.

Background

This is the outcome of the trial in the action brought by Samsung, as claimant, in which it sought a declaration that three of its Galaxy tablet computers did not infringe a Community Registered Design belonging to Apple (the defendant). Apple had counterclaimed for infringement. The validity of the Community Design Registration was not at issue in this case; however, Samsung has separately applied to revoke the registration at OHIM therefore raising issues as to whether the proceedings should be stayed.

In earlier proceedings on this issue in Germany, the Court of Appeal in Dusseldörf held that the Samsung tablets did not infringe, overruling the German first instance court decision. The German Court of Appeal did however grant an injunction on the Samsung tablets based on the German law of unfair competition. In the Netherlands Apple also lost its first instance decision and appeal. However, both the German and Dutch proceedings were preliminary, and therefore this UK action was the first substantive hearing in the Community of the issue of infringement.

Stay of proceedings

The Court considered the issue of whether allowing Apple's counterclaim for infringement (in light of the OHIM proceedings) to continue would open up the possibility of parallel proceedings and a risk of inconsistent judgments on the same point between a Community Design Court and OHIM. The Judge (HHJ Birss QC) noted that Council Regulation (EC) No 2/2002 as interpreted by the Court of Appeal in Samsung v. Apple [2012] EWCA Civ 729, requires the Court to stay the proceedings unless there are 'special grounds' not to do so. The Judge held that the agreement between the parties that the counterclaim should not be stayed; the fact that Samsung had not sought a declaration of invalidity; both sides' agreement that there would, therefore, be no risk of inconsistent judgments between the Community Design Court and OHIM; and that the matter was commercially urgent, were all reasons evidencing 'special grounds' not to stay the infringement counterclaim.

The High Court Judgment

The Court found that the Samsung tablets did not infringe Apple's Registered Community Design, as according to the informed user's overall impression, the Samsung tablets did not have the same understated and extreme simplicity of the Apple design, in effect, "they [were] not as cool" as the Apple design.

The Court stressed that what was important in considering registered design infringement was the registered design, the accused object and the prior art and what these looked like; focusing on the overall impression conveyed to the informed user. The Court noted that although the outcome depends on the overall impression, as a practical matter, the design must be broken down into features. Each feature needing to be considered in three respects (i) a feature dictated solely by function is to be disregarded, (ii) (provided it is not disregarded) the feature must be considered against the design corpus and (iii) this comparison must be considered from the point of view of design freedom.

The Court, applying PepsiCo v. Grupo Promer (C-28/10P) [2012] FSR 5 and Grupo Promer v. OHIM [2010] ECDR 7 held that the informed user was 'a user of handheld (tablet) computers' who, being particularly observant, would consider the Apple and Samsung products side by side. Although the informed user would be interested in the functionality of the products they would also be interested in their aesthetics. It was further stressed that while attention to detail matters, minute scrutiny by the informed user is not appropriate.

The Court considered the following seven features of the Apple design which Apple claimed to be similar in the Samsung products. Within each feature, the Court considered the feature's 'occurrence in the design corpus', 'Samsung Tablets' similarity to the feature' and the 'overall significance of the feature'.

(i) A rectangular, biaxially symmetrical slab with four evenly, slightly rounded corners;

(ii) A flat transparent surface without any ornamentation covering the entire front face of the device up to the rim;

(iii) A very thin rim of constant width, surrounding and flush with the front transparent surface;

(iv) A rectangular display screen surrounded by a plain border of generally constant width centred beneath the transparent surface;

(v) A substantially flat rear surface which curves upwards at the sides and comes to meet the front surface at a crisp outer edge;

(vi) A thin profile, the impression of which is emphasised by (v) above;

(vii) Overall, a design of extreme simplicity without features which specify orientation.

Samsung claimed that many of the above features were the result of limited design freedom and were known in the prior art, and therefore should be given little weight when assessing infringement. Samsung focused on the differences in the design of the

back of their tablets, and their profiles, compared with Apple's Registered Community Design.

The Court noted that for a number of features design freedom was a constraint but that this alone did not account for the close similarity between the products; in fact the similarity was prevalent throughout the design corpus.

Having considered the seven features individually the Court pulled together its findings to consider the overall impression:

'The way the seven features are written; four of them relate to the front of the product, the rear and sides are addressed in two ((v) and (vi)) and the overall position summed up in feature (vii). The front is important but there is a risk of overemphasis. The design is for an object which is hand held and therefore does not simply rest on a desk with its back invisible. The informed user, who is particularly observant, will pick up these objects and will look at the back' (paragraph 179).

'The extreme simplicity of the Apple design is striking. Overall it has undecorated flat surfaces with a plate of glass on the front all the way out to a very thin rim and a blank back. There is a crisp edge around the rim and a combination of curves, both at the corners and the sides. The design looks like an object the informed user would want to pick up and hold. It is an understated, smooth and simple product. It is a cool design' (paragraph 182).

The Court found that, to the informed user, the similar front screens of the two products did not stand-out, as both the Apple design and the Samsung tablets looked like members of the same, pre-existing family. The Court noted that the informed user (who is particularly observant and is informed about the design corpus) would react to the Apple and Samsung design by recognising the front view as one of a familiar type but that as a result, the significance of this similarity overall would be reduced. The informed user's attention would therefore be drawn to the many differences between these products which are to be found at the back and sides and the effect of these would be enhanced considerably. The overall impression produced by the two products in this case was therefore different.

Comment

As stressed by the Court, 'this case illustrates the importance of properly taking into account the informed user's knowledge and experience of the design corpus' (paragraph 189). The weight and importance of a feature that may appear to be similar to the 'uninitiated' can be reduced significantly if in fact the design corpus consistently contains this feature. This case provides a very interesting illustration of how the Court will approach Community design rights infringement. Although such cases are supposed to be simple, as observed by the Court (paragraph 65), often, as in this case, the evidence turns out to be complex and detailed.

Olivia Gray Solicitor
Charters MacDonald-Brown Partner
Redd Solicitors
olivia.gray@redd.eu
charters@redd.eu

Visa/MasterCard Antitrust Litigation

July 2011 saw stakeholders in the long-running antitrust class action against Visa and MasterCard announce a tentative settlement worth more than $7 billion. If approved, the agreement would bring an end to seven years of complex litigation and give class plaintiffs at least some of the remedies they seek.

The suit, initiated by retail merchants and trade associations, requests monetary and injunctive relief against Visa, MasterCard, and their member banks based on allegations that they conspired to charge merchants supra-competitive swipe fees, also known as interchange fees, and imposed anticompetitive restraints in violation of federal and state antitrust laws. Weeks before trial was scheduled to begin, the parties hammered out a settlement that many class plaintiffs considered tolerable. However, now a growing number appear ready to reject the deal.

Background

Visa and MasterCard are bank-card networks comprised of member banks and financial institutions, including Bank of America, Citibank, HSBC, Suntrust, and Wells Fargo, among others. Each network facilitates commerce by allowing cardholders to make noncash purchases using a debit card, charge card, or credit card. A typical transaction involves four players:

- The cardholder;
- The retail merchant;
- The issuing bank, the member bank that issued the cardholder's Visa or MasterCard; and
- The acquiring bank, the member bank that acquires the merchant's payment card receivable and works with the network and issuing bank to settle the transaction.

To illustrate, a cardholder who purchases an item for $100 can pay with a debit or credit card. To make a debit purchase, the cardholder swipes a debit card at the merchant's payment card terminal and enters a Personal Identification Number or PIN into a number pad. If purchasing on credit, the cardholder swipes a credit card and, if required, enters the ZIP code for his or her billing address. Transaction and cardholder information is then transmitted electronically to the acquiring bank, which forwards it to the relevant payment card network. The network, in turn, routes the information to the issuing bank, which confirms the data and determines whether the cardholder has sufficient funds or credit for the transaction. If so, the issuing bank accepts the transaction for the amount of sale ($100.00) less a swipe fee (e.g. 1.65%). The issuing bank's authorisation is then transmitted with a net payment (e.g. $98.35) through the network to the acquiring bank. The issuing bank covers that payment by deducting the amount of sale from the cardholder's checking account or billing it to the cardholder's credit card. On the other side of the transaction, the acquiring bank earns its payment on the sale by guaranteeing that the merchant receives the amount of sale less a merchant-discount fee (e.g. 2.10%), which includes the swipe fee as well as the acquiring bank's fee. Having received the issuing bank's net payment (e.g. $98.35), the acquiring bank then deducts its percentage (e.g. 0.45%) and forwards the balance (in this example, $97.90) to the retail merchant.

The Antitrust Case

In 2005, the class action plaintiffs filed suit to challenge the networks' interchange fees and certain of the networks' allegedly anticompetitive rules. Multiple suits filed in federal court were eventually transferred for centralised pretrial proceedings in the Eastern District of New York. In 2009, a consolidated complaint was filed on behalf of the putative plaintiff class alleging that the defendants had engaged in an illegal conspiracy to fix supracompetitive swipe fees and impose unlawful restraints on trade in violation of the Sherman Act, 15 U.S.C. §§ 1 and 2, and an analogous California law, the Cartwright Act.

First, the class plaintiffs alleged that the networks' uniform fee schedule for interchange fees was the result of horizontal price-fixing agreements among and between Visa board members, MasterCard board members, and major financial institutions that were represented on the Boards. According to the complaint, the inflated swipe fees established in the uniform schedules resulted in market distortion because the fees did not account for the range of risks and processing costs associated with payment methods.

To support their claims, the plaintiffs alleged the basic characteristics of an efficient market. In an efficient market, they claimed, a lower interchange rate would apply to electronic debit transactions, which require entry of a PIN and involve almost immediate deductions from the cardholder's checking account. For these transactions, risks of nonpayment and fraud are minimal. By contrast, a higher swipe fee would apply to transactions involving premium credit cards - exclusive payment cards that offer incentives and benefits such as cash back, mileage points or travel upgrades. Premium credit card transactions carry greater risks of nonpayment because the cardholder, who is billed weeks later, may not be able to cover the balance when it becomes due. The transactions are more costly due to the benefits the card offers. Allegedly, the networks' uniform schedule for default interchange concealed these and other costs from the cardholder. The plaintiffs claimed that cardholders with more complete

information might opt for less costly payment methods, which would reduce the retailer's payment card expenses and pave the way for greater cost savings to consumers.

Second, the class plaintiffs alleged that the networks propped up their inflated swipe fees by establishing and enforcing anti-steering rules that prevented merchants from directing cardholders toward less costly payment methods. For example, plaintiffs challenged Visa and MasterCard's 'No Minimum Purchase Rule,' which allegedly prohibited merchants from imposing minimum purchase amounts for payment card transactions. According to plaintiffs, the networks opposed minimum purchase requirements because they encourage low-dollar cash transactions and, thereby, reduce the merchant's total swipe fees as well as the issuing bank's corresponding profit.

Another rule, the 'No Surcharge Rule,' allegedly precluded merchants from adding a surcharge to payment card transactions based on differences in transaction costs. Plaintiffs claimed that the rule effectively prohibited retailers from passing on discounts for less expensive payment methods. According to the plaintiffs, consumers using more efficient payment methods (e.g. debit cards) were forced to subsidise the least efficient methods (e.g. premium credit cards). The plaintiffs claimed that normalising transaction costs in this way deprived consumers of any incentive to reduce swipe fees charged to the merchant.

At the close of discovery, the class action plaintiffs had reviewed more than 50 million pages of documents and deposed more than 400 witnesses. Roughly two months before trial was scheduled to begin, the parties filed a Memorandum of Understanding ('MOU') with the court stating their intent to settle.

The Settlement Agreement

Under the settlement, the class action plaintiffs will receive roughly $6 billion in damages. Visa will pay $4 billion and MasterCard $2 billion. In addition, Visa and MasterCard agreed to reduce applicable interchange or swipe fees to issuer banks by 10 basis points, but only for an eight-month period following settlement. The temporary reduction in swipe fees is worth about $1.2 billion. Notably, the settlement will allow merchants to add surcharges to payment card transactions in accordance with rules set forth in the agreement. For example, if a retailer adds a surcharge to a Visa card transaction, the merchant must add a surcharge to every payment card transaction with the same or higher cost of acceptance. In return for these concessions, Visa, MasterCard and their member banks will be released from all present and future claims related to the networks' interchange fees and related rules. If twenty-five percent or more of the cash settlement would otherwise go to stakeholders who opt out of settlement, the defendants may terminate the agreement.

Since the MOU was filed, retailers have been reviewing the settlement to determine whether they will accept the proposal or opt out. Some merchants and groups objected to the deal early on, including Wal-Mart, Target, and the National Association of Convenience Stores. Other retailers are now signaling their opposition as well, including members of the National Home Furnishings Association and National Retail Federation, which recently announced it would try to block the settlement. They complain that the $7 billion settlement represents a fraction of the overpayments retailers have been making for years. Not only that, the 0.1% reduction in default interchange is only temporary. After the eight-month period lapses, nothing in the agreement will prevent Visa and MasterCard from returning to current default rates or even increasing them.

Others caution that a retraction of the 'No Surcharge Rule' will be of no consequence in ten states that disallow surcharges on payment card transactions, including New York, California, and Florida. Merchants in other states are not likely to add surcharges. For one, many retailers that accept Visa and MasterCard also accept American Express, which reportedly requires merchants to treat all electronic transactions the same. Under American Express's rules, a merchant that adds a surcharge to credit card transactions must also surcharge debit card transactions. But complying with that rule would violate Visa and MasterCard rules, which prohibit surcharges on debit transactions. Secondly, retailers fear that adding surcharges in this economy will put another drag on sales.

Consumer advocates complain that the settlement transfers wealth from banks to merchants, not to consumers who have been paying higher retail across the board to cover the inflated interchange rates. Although the parties will probably finalise the agreement, it is possible that sufficient numbers will opt out to scuttle the deal. If they do, the class action plaintiffs may get their day in court after all.

Michelle W. Cohen Partner
Jeffrey R. Hamlin Counsel
Ifrah Law PLLC
Michelle@ifrahlaw.com
JHamlin@ifrahlaw.com

FTC v. HireRight Solutions, Inc. and FTC v. Google Inc.

The US Federal Trade Commission declared its intention to increase scrutiny of data brokers and screening companies in March, and has enacted this statement through two cases in which it investigated violations of the Fair Credit Reporting Act and the Federal Trade Commission Act respectively.

As evidenced by several high value settlement decrees it has entered, the United States Federal Trade Commission (FTC) has reasserted itself as a federal agency of which employers and consumers of background information should be aware. Of note, on 8 August in US v. HireRight Solutions, Inc. , the FTC settled a $2.6 million claim with HireRight Solutions, Inc., an employment background screening company, for perceived violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681s(a) (the FCRA). Then, on 9 August, the FTC fined Google, Inc. a total of $22.5M for what it determined was Google's deceptive trade practices in violation of the Federal Trade Commission Act (the FTCA) linked to tracking cookies placed in Apple's Safari Internet browser and Google's breach of a previous settlement agreement with the FTC. Each of the settlement awards obtained by the FTC represent some of the largest awards the agency has ever recovered for violations of the FCRA or the FTCA.

HireRight

In the HireRight matter, the FTC alleged that HireRight Solutions, as a data broker, regularly sold consumer information under the FCRA by providing background reports to thousands of employers throughout the United States to assist them in making hiring decisions. Claiming that the background reports, which included criminal background history of certain individuals, were consumer reports under the FCRA, the FTC argued that HireRight failed to follow reasonable procedures to assure the information furnished was correct. The FTC additionally alleged in its complaint that HireRight failed to disclose to consumers, upon request, all of the information maintained in their consumer report files, failed to conduct reinvestigations of the accuracy of the information in a consumer's file upon the company's receipt of a notice of dispute from a consumer, and failed to maintain strict procedures to ensure that the public record information in the reports was complete and timely at the time the information was reported.

The FCRA regulates the collection, dissemination, and use of consumer information in the United States, including consumer credit information, which is broadly defined under the statute and includes personally identifiable information about background employee data and applicant criminal records. Under the statute, a consumer report is any written, oral, or other communication of any information by a consumer reporting agency that bears on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for among other things, employment. Under the FCRA, employers that request background reports for potential employees must notify the individuals of their rights under the FCRA. If any adverse action is taken against a potential employee based on the results of a consumer report, i.e. a job is not offered, the employer must provide to the individual a copy of the report and a description of the employee's rights under the act.

As employers increasingly rely on data brokers and credit reporting agencies to conduct background checks of potential employees, they are suggested to review their background check policies and practices for legal compliance along with those of their background check providers. Employer use of background reports is increasingly under review by state and federal authorities. Employers that have failed to comply with the FCRA's procedures in obtaining background reports regarding employees have also been sued and faced liability in several lawsuits in the past several years.

Moreover, recently-issued enforcement guidance from the Equal Employment Opportunity Commission also provides that any employer seeking a criminal background check of a potential employee must engage in an individualised assessment of that individual to determine whether a background check is required. Employers also may want to look more closely at the methodologies their screening companies employ, and related representations made in service agreements, to ensure their vendors meet and continue to meet the increasing scrutiny on the screening process.

Google

While addressing a different issue, the FTC's action in FTC v. Google II is further illustration of the FTC's enforcement push. In FTC v. Google II, the FTC alleged that Google had improperly represented to Google users that it would not place tracking cookies in Apple's Safari internet browser but actually did so by using a 'doubleclick advertising cookie' to serve targeted advertisements to users who visit Google websites. According to the FTC, Google used code that was invisible to users to communicate with Apple's Safari browser, thereby setting an unknown cookie on the browser despite Apple Safari's default settings, which do not accept third-party cookies without user

consent. The FTC alleged that Google's representations and actions violated a previous consent decree the FTC had entered with the company, which barred Google from misrepresenting the extent to which consumers could exercise control over their information collection. The FTC found such practice to violate the FTCA as a deceptive consumer practice.

Under the FTCA, the FTC is charged with preventing 'unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce,' which are unlawful under the act. The FTC voted 4-1 to approve the consent decree, which remains subject to court approval under the FTCA. Commissioner J. Thomas Rosch dissented on the basis that Google's non-admission of any liability was not in the public interest and that the $22.5 million settlement award was *de minimis* in light of Google's size and market reach. The remaining commission members voted to approve the consent decree on the basis that the 'FTC staff's careful investigation in this case clearly demonstrated that the historic $22.5 million fine is an appropriate remedy for our charge that Google violated a Commission order by misrepresenting to Safari browser users how to avoid targeted advertising by Google.'

The FTC's action against HireRight and Google is consistent with the agency's announcement in March of this year to increase its enforcement efforts and scrutiny of screening companies and data brokers. The FTC is the enforcement authority for a total of 33 laws including the FCRA, the FTCA, the Telemarketing Fraud and Abuse Prevention Act and the Children's Online Privacy Prevention Act. In light of the recently enacted Dodd-Frank Act, the FTC now shares FCRA enforcement jurisdiction with the Consumer Financial Protection Bureau. As of July 2012, the FTC is also the primary US enforcement agency for privacy violations asserted under the Asia-Pacific Economic Cooperation Cross Border Privacy Rules. As of May 2011, the FTC has brought 32 actions against 'organisations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information.'

More actions by the FTC are expected in the coming year in light of its announced enforcement efforts.

Nick M. Beermann Partner
Jackson Lewis LLP
beermann@jacksonlewis.com

Netflix Privacy Litigation and Missaghi v. Blockbuster LLC

Recent settlements in the US highlight the use of the Video Privacy Protection Act as a Class Action vehicle against the misuse of customers' personal data within the video rentals industry.

The US Congress enacted the Video Privacy and Protection Act, 18 U.S.C. § 2710, et seq. ('VPPA') in 1988 as a reaction to the leak of Supreme Court nominee Robert Bork's video rental records. The VPPA limits disclosure of personally identifiable information by a 'video tape service provider.' A video tape service provider is in turn 'any person, engaged in the business...of rental, sale or delivery of prerecorded video cassette tapes or similar audiovisual materials.' Under the VPPA, service providers may only retain information regarding a consumer for one year and may only disclose personally identifiable information that includes that person's viewing history with the consumer's written consent. The VPPA permits any person aggrieved by a violation to bring a civil action for damages in a federal court.

Indeed litigants have lately been availing themselves of this remedy, and a spate of VPPA class action suits against service providers have been brought in the last year, including notably the case against Hulu, wherein the court recently ruled that Hulu qualifies as a video service provider notwithstanding that it does not rent physical media, but instead streams content over the internet. But the import of the digital age is not the only thing on the minds of class action litigants these days. The Seventh Circuit recently dismissed a case against video rental vendor Redbox, and this summer, federal District Courts preliminarily approved settlements in two significant class actions brought against traditional service providers under the VPPA, In re: Netflix Privacy Litigation (5:11-CV-00379, N.D. Ca.) and Missaghi v. Blockbuster, LLC (Civil No. 11-2559, D. Minn.).

On 5 July 2012, Judge Edward Davila of the Northern District of California preliminarily approved a $9 million settlement in a class action suit against Netflix, the popular on-line and video rental by mail service.

The putative class action suit was brought by former Netflix subscribers, Jeff Milans and Peter Comstock purporting to represent a class of '[a]ll individuals and entities in the United States and its territories that have cancelled their subscriptions to Netflix's services.' The first action was brought against Netflix in January 2011 by Mr. Milans, and several similar suits followed, including Bernal v. Netflix, Inc., Case No. 11-CV-00820-EJD (N.D. Cal.), Rura v. Netflix, Inc., Case No. 11-CV-01075-SBA (N.D. Cal.), Comstock v. Netflix, Inc., Case No. 11-CV-1218-HRL (N.D. Cal.), Sevy v. Netflix, Inc., Case No. 11-CV-1309-PSG (N.D. Cal.), and Wizenberg v. Netflix, Inc., Case No. 11-CV-01359-HRL (N.D. Cal.). The Court consolidated these six cases on 12 August 2011 under the caption In re: Netflix Privacy Litigation and appointed Jay Edelson of Edelson McGuire, LLC as interim lead Class Counsel.

The consolidated class action complaint was filed on 12 September 2011 and challenged the way Netflix retained and used its subscribers' viewing histories and alleged that Netflix violated the VPPA by retaining customer viewing histories longer than 'necessary for the purpose for which [they were] collected.' The plaintiffs alleged Netflix kept information of former subscribers on its servers for more than two years after the subscribers cancelled their accounts and that the information Netflix retained amounted to a 'veritable digital dossier on thousands, if not millions, of former subscribers.' Specifically, the plaintiffs alleged that Netflix kept their viewing histories, credit card numbers, and billing and contact information. Further, the plaintiffs alleged that Netflix violated the VPPA by using the information for marketing and advertising without obtaining the 'informed, written consent of the consumer at the time disclosure is sought' and without providing them 'with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure.' The plaintiffs also alleged that Netflix's retention and use of their information violated provisions of California law.

The parties reached a settlement in March after mediation with retired US District Judge Layn R. Phillips. Netflix did not admit fault, but agreed to decouple former subscribers' rental history from subscribers' identification data one year after cancellation of their service and further agreed to pay $9 million to establish a common settlement fund, out of which class fees and settlement expenses will be paid. The Parties agreed that Netflix would not oppose the plaintiff's request for attorney's fees up to $2,250,000. The balance of the fund will be distributed to *cy pres* recipients, who will be non-profit organisations that educate on privacy issues. The settlement provided that the six named plaintiffs could seek a combined incentive award of $30,000.

Judge Davila noted that in granting preliminary approval he was required to consider whether '(1) the negotiations occurred at arm's length; (2) there was sufficient discovery; (3) the proponents of the settlement are experienced in similar litigation; and (4) only a small fraction of the class objected.' In considering whether the claims were appropriate for class treatment, Judge Davila further noted the requirements of Federal Rule of

Civil Procedure 23. Concluding that all criteria as to both the settlement and class status were met, the Judge certified a class for settlement purposes estimated to be 'tens of millions' of current and former subscribers. In doing so, he noted that the settlement appeared to be 'fair, non-collusive and within the range of possible final approval.' Judge Davila noted that preliminary approval of the settlement was particularly appropriate in light of the immediate injunctive relief that would benefit the class and the minimal monetary recovery that would be available to class members. Further, in justifying its findings, the court referred to the *cy pres* settlements in recent privacy class actions against Google and Facebook, which settled for $8.5 million and $9.5 million, respectively.

Under the settlement agreement, notice to class members was provided through email and publication. A settlement website, videoprivacyclass.com, was also established pursuant to the agreement to provide notice and information to class members and potential *cy pres* recipients. Class members may opt out of the settlement by notice post-marked by 14 November 2012, the same day by which any settlement objections must be filed. A hearing on the final approval of the class action settlement will be held on 5 December 2012.

Likewise, on 8 August 2012, Judge John R. Tunheim of the District Court of Minnesota preliminarily approved a settlement in a class action brought under the VPPA against Blockbuster in Missaghi v. Blockbuster, LLC (Civil No. 11-2559). As with In re: Netflix, the suit alleged on behalf of all current and former Blockbuster subscribers that Blockbuster violated the VPPA by keeping a 'virtual digital dossier' on former subscribers in keeping their viewing histories and personal data, including credit card numbers for more than one year. And like In re: Netflix, the plaintiff's counsel was Jay Edelson.

The suit was filed on 6 September 2011. Blockbuster filed a motion to dismiss. According to the allegations of the complaint, Blockbuster argued, it was in fact a predecessor to Blockbuster LLC - Blockbuster, Inc. - that had collected the plaintiff's personally identifiable information. Blockbuster LLC argued that it could not be liable for the claims the plaintiff alleged because it purchased the assets free and clear of all liabilities out of the Chapter 11 bankruptcy proceedings filed by the old Blockbuster.

After Blockbuster filed the motion to dismiss, the parties engaged in multiple mediation sessions in front of Martin Quinn of JAMS. Unable to resolve the case immediately through mediation, the parties engaged in additional settlement discussions before arriving at an agreement in April. The motion to dismiss was pending at the time the parties reached an agreement and was withdrawn on 2 July.

Finding that the criteria for fairness and class treatment were satisfied, Judge Tunheim's preliminary approval order certified a class of '[a]ll current and former "Blockbuster" members in the United States and its territories and possessions' for purposes of settlement and preliminarily approved the settlement agreement. Unlike the Netflix settlement, the Blockbuster settlement did not provide for a monetary recovery. Rather, Blockbuster has agreed to modify its privacy policy to state that all accounts continue unless they are affirmatively terminated, notwithstanding its denial of liability. Blockbuster further agreed to create a process for former subscribers to request to have their personal information deleted from the company's database. The settlement also provides for Blockbuster to pay $140,000 in fees to class counsel.

Under the settlement, notice was provided to class members by publication in USA Today on two consecutive Mondays. Objections to the settlement are to be filed by 26 October 2012, and a fairness hearing on the settlement will be held on 27 November 2012.

While VPPA suits were certainly a hot topic over the last year, it remains to be seen whether the VPPA will continue to be a favoured vehicle for class action litigants in 2013. In December 2011, the House of Representatives easily passed a bipartisan measure to amend the VPPA, H.B. 2471. The bill, introduced by Bob Goodlatte (R-VA), Howard Coble (R-NC), Jim Sensenbrenner (R-WI) and Linda Sánchez (D-CA), would amend the VPPA to allow service providers to obtain consumers' informed, written consent '[i]n advance for a set period of time or until consent is withdrawn.' In addition, H.B. 2471 enables consumers to give their 'informed written consent' electronically over the internet.

Erica Gann Kitaev Partner
BakerHostetler
ekitaev@bakerlaw.com

E-land v. Taobao

The First Intermediate Court of Shanghai

A number of key e-commerce cases are clarifying China's e-commerce laws. One of which was the First Intermediate Court of Shanghai's ruling that Taobao, China's largest online marketplace, was liable for 'contributory infringement'.

The E-Land v. Taobao case in China is similar to the L'Oreal v eBay case in the EU. In the E-land case the Chinese courts found Taobao (the e-commerce operator) to be jointly liable for the infringing act of its platform user. In this case, E-Land, the trademark holder of a popular Korean fashion line, had filed numerous complaints of trademark infringement with Taobao since 2006. From September to November 2009, E-Land filed seven 'take down' notices to Taobao against seller Du Guofa. Taobao deleted web links upon receipt of the take down notices. In July 2010, E-Land filed a case against Du Guofa and Taobao for the trademark infringement and in September 2010, Taobao deducted points from Du Guofa's account as a penalty.

In a previous 1996 case against Taobao by Puma AG in similar circumstances, the Guangzhou Intermediate Court refused to accept that Internet Service Providers (ISPs) are obliged to check whether persons using their services have a legitimate right to do so. In January 2011, the Shanghai Pudong People's Court found that Du Guofa and Taobao's acts constituted infringement and were both held liable. The Court found that although Taobao did eventually remove the infringing material upon notice, it was fully aware of Du Guofa's infringing acts and did not take effective measures against it.

On appeal, in April 2011, the Shanghai First Intermediate People's Court (the 'Intermediate Court') upheld the first instance court. The Intermediate Court reasoned that Taobao should have been aware of the infringing goods being sold as it had received numerous complaints from E-Land since 2006. As of 2009, since there were still a lot of counterfeit goods being sold on E-land's website, Taobao should have known that its method of deleting the web links was not effective. The Intermediate Court considered that by only 'passively' deleting links to counterfeit goods when users continued to commit infringements and not taking more effective measures to prevent the infringement from persisting, Taobao had promoted and encouraged the infringing acts and as a result, constitutes 'contributory infringement'. Taobao was ordered to pay compensation of RMB 10,000.

It is worth noting that if a person is found to have used a trademark without authorisation, the infringer under China's Anti-Unfair Competition Law can also be required to reimburse expenses incurred by the rights holder for investigating unfair competition. In the Taobao case, no claim was made for reimbursement of such expenses.

2011 Joint Agency Circular

Also, in mid-2011, nine Chinese Enforcement Agencies involved in the regulation of e-commerce issued a Circular on 'Further Moving Forward Actions on IP Right Infringement and Manufacture, Sale and Passing-off of Inferior Products in the Online Shopping Sector' (the 'Circular'). This Circular clarifies the duties of online shopping forums. According to the Circular, e-commerce operators are required to:

- establish a trade mark and patent enquiry system;
- adopt technical means to screen information on IP rights infringement and the sale of knock-offs and inferior products;
- establish a 24 hour online inspections system;
- investigate and eliminate hidden dangers in time; and
- handle violations of regulations and laws.

Taobao continues to attract the attention of the Chinese authorities with recent allegations of illegal online auctions, and protests by thousands of small shop owners who objected to an increase of between five and ten times in annual fees by Taobao.

Conclusion

While it may be difficult for rights holders to discover and take action against infringers using e-commerce platforms, in China it is becoming more and more the responsibility of the e-commerce operators to take effective measures against infringing users. Faced with large numbers of infringement complaints, an e-commerce platform will have to assess whether (actual or presumed) knowledge of these infringements is sufficient to justify tough measures against a customer, so as not to result in joint liability itself.

Frank Schoneveld Partner
McDermott Will & Emery
Jia Yau Foreign Counsel
MWE China Law Offices
fschoneveld@mwe.com
jyau@mwechinalaw.com