

# eBUSINESS GLOBAL NEWSLETTER

## OCTOBER 2009

### e-marketing

Poland	(Draft) new spam regulations in Poland	p. 2
The Netherlands	Stricter rules for sending newsletters and telemarketing	p. 3
United States	Rescuecom v. Google: changing the future of keyword advertising in the United States?	p. 5
European Union	No absolute protection in the EU for Google AdWords trade mark infringements	p. 7

### data protection

France	Recommendations for transferring personal data in connection with U.S. discovery procedures	p. 9
United States	Overbroad Maine minors privacy law averted through DLA Piper challenge	p. 11

### e-publishing

UK / US	Cross-border defamation case law: UK - US comparison	p. 12
---------	--	-------

## This month's contributors

- Patrick Van Eecke and Maarten Truyens (Belgium)
- Carol Umhoefer (France)
- Richard van Schaik (the Netherlands)
- Marlena Wach and Dagmara Jaskulak (Poland)
- Duncan Calow and Alan Williams (United Kingdom)
- Christina L. Martini (Chicago, United States)
- Andrew Deutsch (New York, United States)
- Jim Halpert (Washington DC, United States)

## (Draft) new spam regulations in Poland

The Polish legislator is working on a new draft telecommunications Act which will also include separate regulation on spam (*i.e.*, unsolicited commercial informations). At present, spam is regulated in the Polish Act on Electronic Services of 18 July 2002.

### Background

Initiatives to regulate spam have already started on 2006. The Polish legislator could not decide whether there should be a separate act on spam, or whether it should be included in telecommunication law or regulations on electronic services. Therefore, even though spam deserves a new regulation, it is difficult to foresee when the new regulation will be enacted — particularly due to the fact that the new regulation is negatively perceived by telecommunication operators and providers of telecommunication services, mostly because it imposes several new obligations on them.

### Content of the (draft) new regulation

As is the case with the present regulation, the new regulation requires prior consent for sending any commercial information (the “opt-in” model). However, the new regulation introduces a much broader definition of spam, also covering messages for which the context and content is independent from the recipient, messages sent by automated calling system for direct marketing purposes, messages intended to create contact databases (in particular for marketing purposes) and also commercial information, as defined in the Polish Act on Electronic Services (any information designed to directly or indirectly promote the goods, services or image of a company or person exercising a regulated profession, excluding information enabling communication by electronic means that is not designed to cause a commercial effect, and in particular sent with no intent of remuneration or other benefits by manufactures, sellers and persons rendering services).

According to the new draft, messages and commercial information should identify the sender and its correspondence address (or indication where such informa-

tion may be obtained). Furthermore, the recipient must also be informed about the right to withdraw his/her consent.

Contrary to the present regulation, where spam is subject to criminal proceedings, the new regulation gives the President of the Office of Electronic Communication (National Regulatory Authorities - NRA) the right to commence administrative proceedings in order to impose financial penalties for sending spam. The aim of this change is to improve the effectiveness of fighting with spam.

The new regulation also introduces the idea of a so-called “spam box”. The President of the NRA will be obliged to establish a national complaint desk for the purpose of reporting spam, in order to collect and process information necessary for anti-spam proceedings, to detect and eliminate spam, and to facilitate the international cooperation against spam. Telecommunica-



tion service providers will be obliged to also establish their own complaint desks, in order to investigate spam incidents, enable the subscriber to report the spam and to cooperate with other telecommunications services' providers.

Furthermore, a provider of telecommunication services that detects spam will be obliged to locate where the spam was sent from. In such situation, the provider will also be obliged to notify the subscriber who sent the spam, and to provide him/her with clear instructions on how to avoid sending spam again (*e.g.*, remove spyware installed on his/her pc). Additionally, if this is technically possible, the provider must supply the subscriber with appropriate software. The subscriber will then be obliged to remedy irregularities within two days from receiving information from the telecommunication services provider. In case the subscriber does not remedy the irregularities, the provider will be allowed to limit the connection speed to 32 KB/s (incoming) or 16 KB/s (outgoing) until the subscriber removes the irregularity. In case the subscriber removes the irregularity within seven days from notification, restoring the connection speed is free of charge. The new regulation also imposes information obligations on the telecommunications

services providers, who will have to report to the NRA all information regarding detected spam, personal data of the subscribers and information about undertaken actions. Furthermore, the provider should also report to NRA information about spam sent from outside of the territory of Poland.

The new regulation introduces much higher penalties for sending the spam, which will amount up to PLN 100.000 (approximately EUR 24,000). Additionally, the providers who did not report information required by the NRA, who did not limit the connection speed or who did not establish a complaint desk will be subject to penalty of up to PLN 5.000 (approximately EUR 1,200).

### Legislative process

The new regulation is subject to internal discussions within the Ministry of Infrastructure. It has to be accepted by Legal Commission at the Council of Ministers and by Council of Ministers and later has to go through the legislative procedure at the Parliament. Due to the negative reactions of the telecommunication market, it is expected that public discussion on the regulation will be very intense and may prolong enacting process. ■

## e-marketing • the Netherlands

# Stricter rules for sending newsletters and telemarketing

On 1 October 2009, adjustments to the Dutch Telecommunications Act came into force. One of the main changes is that sending newsletters in the Netherlands via e-mail is subject to stricter rules. In addition, the "Don't Call Me" Register was introduced, which has important consequences for the telemarketing business.

### Spam prohibition

The definition of "spam" is "*unsolicited communication via fax or electronic messages (e-mail, text messaging) for commercial, ideological or charity purposes*". Before 1 October 2009, it was prohibited to send this type

of communication in business to consumer relations, except in case prior consent was given (opt-in regime). Due to the recent changes, this prohibition has been extended to business to business relations. This means, for example, that the main rule for sending out all newsletters for commercial, ideological or charity purposes, is that prior consent is required from all receivers for such newsletters.

The prior consent must be specific and informed, which means that the addressee should understand the purpose for which he grants his consent. This can for example be

done by actively ticking a box on a webpage. Note that specific permission means, that it cannot be obtained by mere reference to the terms and conditions.

## Exceptions

An important exception to the foregoing opt-in regime applies to existing customers. It is allowed to send them electronic messages, provided that the following conditions are met:

- details must be obtained within the framework of the sale of the sender's own products and services (it does not cover purchase of a database from a third party);
- the newsletters and other means of communication must refer to the sender's own and similar services and products as those for which the electronic contact details were gathered initially;
- when gathering the electronic contact details of the addressee, the latter must be offered the possibility to object free of charge against the use of his details (*i.e.*, to opt-out). Moreover, this possibility should be offered for each individual communication.



Besides the abovementioned exceptions to the spam prohibition, the Telecommunications Act also provides for an exception regarding addressees based outside the European Economic Area (unless such is prohibited by local law), as well as for contact details specifically created for receiving unsolicited e-mails, such as *marketinginfo@companyname.com*.

## Don't Call Me Register

Another change in the Telecommunications Act is the introduction of the Don't Call Me Register. This change is only effective for natural persons. If they do not wish to be approached for telemarketing purposes (unsolicited telephone calls to sell products or services), they can include themselves in this register. Again, an exception to this rule applies to existing customers, inasmuch as the sale by telephone is aimed at the sale of the sender's own similar products and services (or donations to ideological institutions or charities).

Also, in the event explicit permission has been granted for certain forms of telemarketing, it is allowed to call, regardless of the fact that the person in question is included in the Don't Call Me Register. If a participant to a certain action for example checks a box that he consents to being approached (by telephone) for marketing purposes, then this (special) permission prevails over the (general) opt-out of the register. However, in case a company will call such a person, he still must be pointed to (the possibility of inclusion in) the Don't Call Me Register, and also to opt out the further use of his details.

Since we just passed 1 October, please note that if you would like to send newsletters to potential or existing customers, make sure that you will act in compliance with the new legislation. Therefore, check your policy in relation to commercial communications. If you are using call centers to sell your product, be advised to make clear agreements on these new rules. In case you would like to send your newsletter per email ask for consent if necessary! ■

## Rescuecom v. Google: changing the future of keyword advertising in the United States?

*For the past several years, keyword advertising has been a highly lucrative, multibillion-dollar industry—one that, not surprisingly, has triggered a significant amount of controversy. Does the use, purchase and sale of trademarks as keywords constitute trademark infringement?*

Courts have not answered this question predictably. On April 3, 2009, in a long-awaited decision, the Second Circuit Court of Appeals rejected the district court's dismissal of a trademark infringement action brought against a search engine by a national computer service franchising company. *Rescuecom v. Google*, 562 F.3d 123 (2d Cir. 2009). In *Rescuecom v. Google*, the Second Circuit has in effect reversed its prior position on the keyword issue by rejecting the lower court's findings and holding that Google's recommendation and sale of the RESCUECOM trademark as a keyword to plaintiff's competitors constitutes use of the trademark "in commerce." There is still a split in the circuits on this issue, but the Second Circuit now follows the majority view. The case is currently remanded to the district court. If ultimately decided on the merits, *Rescuecom v. Google* will likely have a profound impact on search engines and the keyword advertising industry.

### Background and the District Court

Rescuecom conducts a large amount of its business over the Internet, and many of its competitors advertise on the Internet using tools offered by various search engines, including Google's AdWords program. Google, through its Keyword Suggestion Tool, recommends the RESCUECOM trademark and, through its AdWords program, offers this keyword for sale to Rescuecom's competitors. When a Google user searches the term "Rescuecom," links to competitive websites appear on the user's screen.

Rescuecom brought claims against Google alleging trademark infringement, false designation of origin and trademark dilution. In its complaint, Rescuecom alleged that Google's sale of the RESCUECOM trademark as a keyword causes confusion by diverting Internet users to competitors' websites.

The United States District Court for the Northern District of New York granted Google's motion to dismiss on the basis that its use of the RESCUECOM trademark is not a "use in commerce," and therefore does not constitute trademark infringement. *Rescuecom v. Google*, 456 F. Supp. 2d 393 (N.D.N.Y. 2006). Relying on the Second Circuit's decision in *1-800 Contacts, Inc. v. WhenU.com, Inc.*, the court held that the sponsored links triggered by Google's keyword tool did not



The image shows a screenshot of a Google search interface. At the top left is the Google logo. To its right is a search box containing the text "rescuecom". Below the search box is a "Web" tab and a "Show options..." link. The search results are displayed below, starting with a link to "Computer Repair | Computer Support | RESCUECOM provides Fast and Flawless Computer Repair - RESCUE-PC (1-800-737-2837) Laptop Repair - Virus Removal - Satisfaction Guaranteed". Below this is the URL "www.rescuecom.com/" followed by links for "Cached", "Similar", and a speech bubble icon. At the bottom of the screenshot, there is a snippet from a document dated "18 Aug 2009" with the text "... RESCUECOM's Computer Repair - statistical ... RESCUECOM Computer Repair - www.rescuecom.com/RESCUECOM269".

actually reference the RESCUECOM trademark. See *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 414 F.3d 400 (2d Cir. 2005). Thus, the court concluded that Google’s use of the RESCUECOM mark was not a “use in commerce” under *1-800 Contacts*, which held a company’s private internalization of a trademark in its ad-triggering software is not a “use in commerce.” *Rescuecom* appealed the decision.

## Second Circuit Opinion

The Second Circuit reversed the dismissal, held *Rescuecom*’s complaint properly alleged a claim for relief and noted two significant distinctions from *1-800 Contacts*. Specifically, in *1-800 Contacts*, plaintiff’s website address, not its trademark, triggered the pop-up advertisement at issue. In fact, the case’s dictum suggests that use of plaintiff’s trademark to trigger the pop-up advertisement may have been actionable. Moreover, the advertisers in *1-800 Contacts* could not purchase trademarks as keywords. By contrast, in *Rescuecom*, Google encouraged the purchase of the plaintiff’s trademark through its Keyword Suggestion Tool, displayed, offered and sold the mark through its AdWords program, and controlled advertisement placement through the keyword itself.

The Second Circuit also rejected Google’s contention that including a trademark in an internal computer directory in its ad-triggering software does not constitute trademark use. It found that Google’s recommendation and sale of the RESCUECOM trademark to its advertising customers was not an internal use and, even if it was, such a finding would not preclude a “use in commerce.” The court concluded that *Rescuecom*’s complaint properly alleged a claim for relief and remanded the case to the district court to decide the merits of the trademark infringement and related claims.

## Potential Impact of the *Rescuecom* Decision

Prior to *Rescuecom*, several district courts in the Second Circuit followed *1-800 Contacts* and held that neither the internal use of a trademark to trigger sponsored links, nor the purchase of a trademark as a keyword, constitute

“use in commerce.” *Rescuecom* is essentially a reversal of the Second Circuit’s decision in *1-800-Contacts*. A majority of the other circuits have already adopted the *Rescuecom* position on the “use in commerce” issue, but a few remain which take the opposite view. Since the district court in *Rescuecom* is now considering the merits of plaintiff’s trademark infringement and related claims, it will hopefully provide more clarity and uniformity regarding the liability associated with keyword advertising.

Because many search engines generate much of their revenue through keyword advertising, *Rescuecom*’s outcome is potentially significant. Before this case, the Second Circuit was one of the few jurisdictions in which search engines were essentially immunized from liability if their use of the trademark was “internal” to their ad-triggering software and not visible to users. Now, under *Rescuecom*, such trademark infringement claims are much more likely to be evaluated on the merits. Thus, defendants are less likely to engage in forum shopping tactics such as filing preemptive declaratory judgment actions in the Second Circuit, and plaintiffs are more likely to file suit there.

Given the high stakes, search engines will likely make significant investments in defending such cases. They also have incentive to explore new technologies that promise to reduce legal risks. Companies may also be more reluctant to promote their businesses through keyword advertising, meaning decreased revenues for both advertisers and search engines.

*Rescuecom* is particularly helpful to trademark owners who seek relief against the unauthorized use of their trademarks in keyword advertising. Although it is unclear whether the district court will ultimately find Google liable for trademark infringement, *Rescuecom* has brought the Second Circuit in line with other courts throughout the country which have given plaintiffs the opportunity to have their day in court. This will likely shape the legal landscape for keyword advertising in a more straightforward way for all interested parties. ■

# No absolute protection in the EU for Google AdWords trade mark infringements

“Googling” has become an established phenomenon that forms an important part of the way in which we access information. Google’s search engine activities are mainly subsidised by its AdWords system, which generated 21 billion dollar in revenues in 2008. This system allows for pay-per-click advertising and offers targeted text and banner ads. Advertisers can bid on keywords so that, following a successful bid, the bidder’s advertisements are displayed to Internet users searching on these keywords. As few restrictions apply to the available keywords, advertisers with less noble intentions can bid on keywords which correspond to established brand names in order to advertise their websites offering counterfeit products of the brand in question.

For some French brand owners – such as the holding LVMH Moët Hennessy Louis Vuitton – this went a bridge too far. They took the matter to court in France. Following a prejudicial question by the French Court de Cassation, their cases (C-236/08, C-237/08 and C-238/08) made their way to the European Court of Justice in Luxemburg.

On September 22, 2009, the opinion of Advocate General (AG) Poiares Maduro was made available to the public. Although the opinion of the AG is not binding, the Court of Justice often follows the reasoning of the opinion of the AG. In many cases, the opinion is therefore a precursor to the court decision.

The opinion deals with three distinct questions. The first question is whether trade mark owners can prevent the use *by Google* of keywords which corresponds to their trade mark. Secondly, it is examined whether trade mark owners can prevent *advertisers* to use keywords corresponding to their trade marks. Finally, the AG considers whether the liability exemption for hosting (introduced by the E-commerce Directive), applies to the content featured in AdWords. If this would be the case, Google

might be exempt from liability for the alleged infringements committed through AdWords.

## I. Use of trade mark keywords by Google

With regard to the first question, the AG considers that trade mark owners cannot preclude Google from using keywords corresponding to trade marks. According to the current case law, four criteria must be met for a trade mark infringement: (1) the use of the trade mark is without the owner’s consent; (2) the use takes place in the course of trade; (3) the use relates to goods or services which are identical or similar to those covered by the trade marks; and (4) the use affects (or is liable to affect) the essential function of the trade mark – i.e. guaranteeing to consumers the origin of the goods or services – by reason of likelihood of confusion on the part of the public.

According to the AG, the first condition (use without consent) is indisputably satisfied, since none of the trade mark owners consented with Google’s use of their trade mark as a key word.

As regards the second condition (use in the course of trade), the AG first distinguishes between two different trade mark uses by Google. The first use is where Google allows advertisers to *select* the keywords, so that ads for their sites are presented in response to searches involving those keywords. The second use is when Google *displays* such ads, alongside the “natural” search results displayed in response to those keywords.

The second condition – use in the course of trade – is fulfilled for both uses, as both the selection of keywords and the display of ads take place in the course of trade.

The difference between the two uses is particularly relevant for the examination of the third condition. The AG argues that the first use (selection of keywords) is not made in relation to goods or services which are identical

or similar to those covered by the trade marks, since no goods or services are sold to the general public through AdWords. The use is then limited to a selection procedure which is internal to AdWords and concerns only Google and the advertisers. Conversely, in the second use (displaying ads), a link is established between the keywords that correspond to trade marks and the goods or services on the advertised sites. The third criterion is therefore satisfied in relation to Google's display of ads.

Finally the AG considered the fourth condition: whether Google's use harms or can harm the essential function of the trade mark, by reason of a likelihood to confuse the public. The AG estimated that for Google's first use (keyword selection), it was unnecessary to analyse this condition, because the use does not involve identical or similar goods or services, so that there can be no risk of confusion by the public. With regard to the second use (displaying ads), the AG argued that a search engine user is sufficiently conscious that several results will be displayed, of which only a handful are relevant to his query. Consequently, the fact that several websites are shown besides the trademark holder's website, will not confuse the consumer. Search engine users will only make an assessment as to the origin of the goods or services advertised on the basis of the content of the ad and by visiting the advertised sites. No assessment will be based on the mere fact that the ads are displayed in response to keywords corresponding to trade marks. Hence, according to the AG, there is no risk of confusion related to this application.

Next, the AG had to examine whether Google's use of trade mark keywords takes unfair advantage of, or is detrimental to, the distinctive character or the reputation of the trade mark. He argues that a registered trademark cannot be used by its owner to prohibit each and every use by third parties, as would be the case with "classical" ownership rights. This trade mark protection has to be balanced against other interests, such as the freedom of commerce and freedom of expression. Some uses – such as the use for purely descriptive purposes and comparative advertising – cannot be prevented by the trade mark owner. The AG estimates that, although Google's use of trade mark keywords does not constitute true comparative or descriptive advertising, creates a link to the trade mark for consumers to obtain information that does not involve a risk of confusion. According to the

AG, keywords are one of the instruments by means of which this information is organised and made accessible to the internet users. Keywords are therefore, in themselves, content-neutral, which precludes the trade mark owners from opposing themselves against it.

## II. Use of trade mark keywords by advertisers

Under the second question, the AG also had to consider whether the use by advertisers of keywords corresponding to trade names would constitute a trade mark infringement. Here, the AG clarified that, contrary to Google's commercial use of keywords corresponding to trade marks, the advertisers' use was private. This private use by advertisers is the flipside of Google's first use (allowing advertisers to select keywords). Accordingly, it would be highly contradictory to consider the advertisers' use an infringement, whereas Google's use of the same keywords is permitted. Such a decision, the AG considered, "*would be tantamount to saying that Google should be permitted to allow the selection of keywords that no one is permitted to select*".

The AG did not want to go as far as considering that the use of a keyword corresponding to a trade mark constitutes, in itself, a trade mark infringement. Such a decision would preclude all the legitimate uses of the AdWords services, such as comparative advertising and product reviews. However, nothing prevents trade mark owners to intervene on a case-by-case basis whenever the effects of ads displayed to users involves a risk of confusion.

## III. Applicability of the liability exemption

The third question was whether the liability exemption for hosting services (as introduced by article 14 of the E-commerce Directive 2000/31/EC) applies to the content featured by Google in AdWords.

For the liability exemption to apply, the AdWords service must qualify as "hosting", i.e. the storage of information, provided by the recipient of the service, at the request of that recipient. Furthermore, the liability exemption only applies to the extent that Google does not have any actual knowledge of the illegal nature of the information, or of facts which would make such illegality apparent. When Google would become aware of illegal information, it must promptly remove it.

The AG concluded that AdWords is not a “neutral information vehicle”, since the ads displayed by Google stem from its relationship with the advertisers. Consequently, as Google’s services go further than mere hosting, the liability exemption does not apply.

## Conclusion

The opinion of the AG is based on the consideration that “it is important not to allow the legitimate purpose of preventing certain trade mark infringements to lead all trade mark uses to be prohibited in the context of cyberspace”. If the AG’s opinion were to be followed by the European Court of Justice, Google would be given

a lot of freedom in running its AdWords service. However, the opinion should not be interpreted as giving Google strong protection. If the AG’s opinion were to be followed by the Court, trade mark owners will still be able to intervene on a case-by-case basis whenever the effects of ads displayed to users involves a risk of confusion. Such an approach, the AG considers, is much more balanced, and does not allow trade mark owners to prevent all possible uses – including many lawful and even desirable uses – of keywords corresponding to trade marks. Of course, it remains to be seen whether the Court of Justice will take a similar view. ■

data protection • France

# Recommendations for transferring personal data in connection with U.S. discovery procedures

For the past several years, the French Data Protection Authority, the “CNIL”, has been focusing on issues relating to transfers of personal data to the U.S. in connection with internal corporate and U.S. government investigations, as well as U.S. discovery proceedings. Transfers of personal data to the U.S. may be problematic in any context due to the fact that the European Commission does not recognize U.S. laws as providing adequate protection for personal data. The problems are compounded in the context of an investigation or discovery proceedings.

The CNIL has now issued a Recommendation<sup>1</sup> with respect to transfers of personal data in connection with U.S. discovery procedures, following a similar opinion issued by the group of EU Member State Data Protection Authorities, the Article 29 Working Party, at the beginning of the year<sup>2</sup>.

Although the CNIL Recommendation marks a major innovation with respect to the legal basis for transfers pursuant to U.S. discovery proceedings, and brings clarity to a number of issues that have stymied companies



and practitioners for several years, there may remain a number of practical dilemmas faced by companies transferring personal data for use as evidence in U.S. civil litigation.

### Progress on several fronts

The Recommendation clarifies several issues, including the duration of conservation of personal data transferred for purposes of U.S. discovery, and the categories of data that may be permissibly transferred.

More significantly, in its Recommendation, the CNIL has taken the bold and novel position that a company may justify a one-off transfer that is not “massive”, on the basis of the company’s legitimate interest in defending its rights in court.

As a consequence of this position, the Recommendation states that no CNIL authorization is needed for one-off transfers that are not massive. Moreover, a literal reading of the French Data Protection Law indicates that in such circumstances, the recipient of the data need not be FTC Safe Harbor Certified, nor party to Model Clauses or Binding Corporate Rules. However, any other transfer in the context of discovery (e.g., repetitive or massive transfers) implies Safe Harbor certification, Binding Corporate Rules, Model Clauses and/or a protective order issued by the U.S. court.

The Recommendation also expressly states that the requirement to inform an individual that his/her personal data is being transferred to the U.S. pursuant to U.S. litigation may be suspended as long as there is a risk that evidence collection could be hampered e.g., through evidence tampering. This is a welcome recognition of a principle that has already found its place in the CNIL’s Single Authorization for whistle-blowing systems<sup>3</sup>.

### Practical difficulties remain

Nonetheless, the practical benefits of the CNIL’s novel position are limited because, as the CNIL rightly notes, in all cases the transfer of personal data is governed not only by the French Data Protection Law, but also potentially by the French Blocking Statute<sup>4</sup>. The Blocking Statute prohibits, inter alia, the transfer of commercial, financial or economic documents or information outside France for the purpose of non-French litigation, unless

such documents or information is transferred pursuant to the Hague Convention<sup>5</sup>. Violations of the Blocking Statute (like the Data Protection Law) are punishable by criminal fines and/or imprisonment.

The ramifications of the application of the Hague Convention are several. Pursuant to a declaration made by France, the scope of U.S. discovery requests directed to France must be limited to documents that have a specific relation to the subject-matter of the U.S. litigation; the documents requested must also be enumerated. Moreover, Hague Convention procedures may delay the production of evidence in U.S. proceedings. Finally, the French judge charged with carrying out discovery requests is empowered to review the relevance of the document requests.

### And investigations?

The Recommendation, although making several references to investigations, does not formally address issues relating to internal or government investigations. It therefore remains to be seen to what extent the Recommendation will be persuasive for French judges who are ruling on disputes related to transfers of personal data pursuant to investigations. ■

#### Notes

<sup>1</sup> Deliberation no. 2009-474, dated July 23, 2009, constituting recommendations relating to the transfer of personal data in connection with U.S. discovery procedures.

<sup>2</sup> Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted February 11, 2009.

<sup>3</sup> Single Authorization AU-2005-004, dated Dec. 8, 2005.

<sup>4</sup> French law no. 68-678, dated July 26, 1968, as amended.

<sup>5</sup> Hague Convention, dated March 18, 1970, on the taking of evidence abroad in civil or commercial matters.

# Overbroad Maine minors privacy law averted through DLA Piper challenge

## Maine legislature prepares to rewrite the law

Last month, DLA Piper US succeeded in a First Amendment challenge in a Maine federal court to an overbroad Maine state law against marketing to or transferring information about minors. The law would have barred parties from collecting any personal information or non-personally identifying health-related information from minors without verifiable parental consent. It would thus have extended U.S. Child Online Privacy Protection Act (COPPA) law national restrictions against collecting personal information online from children under 13 to teenagers and to information collected offline, and would have imposed similar restrictions against Internet advertising using non-personally identifying health-related information.

The law also would have barred any transfer of personal information about minors and barred using information about minors to market any service or product or to recommend any course of action with regard to a product or service. The law would have been enforceable not only by the Maine Attorney General but also by private parties in class action lawsuits of \$250 per individual violation, an amount which could have been tripled in the case of a “knowing” violation.

The named plaintiffs who sued to enjoin the statute were The Maine Independent (private) Colleges Association, The Maine Press Association, Reed Elsevier and NetChoice, a technology trade association. The law was of major concern to a broad range of companies, who helped fund the lawsuit through trade associations.

The State Attorney General’s Office (which defends lawsuits against the state) acknowledged that the law was overbroad and restricted minors’ rights under the First Amendment to receive information. However, after the DLA Piper team filed for a preliminary injunc-

tion against enforcement on First Amendment, Dormant Commerce Clause and COPPA Preemption grounds, the Maine Attorney General (the “AG”) attempted to moot the case by pledging not to enforce the law and arguing that no relief could be obtained either against the AG or potential third-party plaintiffs. After additional briefing over Labor Day weekend, Bruce Falby (B) argued the preliminary injunction motion four days before the law was to take effect.

The DLA Piper team succeeded in convincing District Court Judge Woodcock to issue an order finding that plaintiffs had established a likelihood of success on the merits of their claims that the statute was overbroad and violated the First Amendment; memorializing the AG’s commitment not to enforce the law and the Maine legislature’s intent to revise it; and putting private parties on notice of the constitutional infirmities in the statute. The court then accepted the parties’ agreement to the dismissal of the case without prejudice, pending the Maine legislature’s review and revision of the statute.

The case was a collaboration between DLA Piper’s Washington and Boston offices. Jim Halpert and David Lieber in Washington worked to put the litigation funding and plaintiffs together and worked on the briefs. Bruce Falby, Matt Iverson, Brooks Ames, and Eileen Pott (all in Boston) filed and argued the case.

Maine House Judiciary Committee will hold hearings on how to amend the bill to fix its constitutional defects on October 15th and possibly October 16th. Written comments must be filed with the Committee by October 8th to testify at the October hearing. DLA Piper’s client, the State Privacy & Security Coalition will be filing comments addressing the constitutional and practice issues raised by the sweeping Maine law. ■

# Cross-border defamation case law: UK - US comparison

## I. The UK perspective

London is still considered the libel capital of the world. Accordingly, and despite the weather, it attracts more than its fair share of libel tourists: those people in search of what they perceive to be a claimant-friendly jurisdiction to bring a defamation action against a publisher. (From time to time other cities can look attractive to those on such an excursion. For example, colleagues in Paris often warn us of the ways in which French law can be pro-claimant and one of the leading Internet libel cases was brought in Australia - where perhaps food and climate might be better respectively?).

The essence of UK libel law is that a person is entitled to his or her reputation and that can only be taken away on precise terms. The onus is effectively on the defendant not the claimant to prove their case. Unlike the US, there is no “public figure” defence. A defendant in the UK has either to prove the truth of what he or she has written (and it is the ordinary reader’s understanding of the meaning, not what the author intended, that counts); or demonstrate fair comment or privilege or a number of other lesser-used defences. Prior publication is no defence, though the fact that the libel has been published before may help to reduce any damages awarded.

The UK has also increased in attractiveness through the introduction of contingency fee arrangements (CFA’s), enabling impecunious claimants to find “no-win no-fee” lawyers to bring actions the claimant would not have previously been able to afford.

UK courts have been prepared to accept jurisdiction and try libel cases provided that the offending material has been published here. In the past, just a few copies of a book or magazine being offered for sale could be considered enough. Under UK rules defamation is generally deemed to occur where the offending material is

received and read, not where it was printed or – in a digital world – uploaded or hosted. Only in limited cases have the courts turned away claimants seeking a hearing here. With the development of Internet sales and online publishing there has been an increased ability for material from other countries to reach readers in the UK and, with it, an increased likelihood of libel tourists booking into London hotels.

So claimants have sued foreign defendants in the UK, obtained judgment and (whether the defendant has appeared or not) obtained permission from the London court to take the judgment and seek to enforce it in other jurisdictions. The success of those efforts can vary. In particular, the American courts, with a very different approach to defamation law have always been chary of allowing English defamation judgments to be enforced in the United States. The recent Mahfouz case, the latest in a line of cases, has, however, stimulated even greater reaction.

In 2004, the Saudi billionaire Khalid bin Mahfouz launched a libel action against Rachel Ehrenfeld, the author of a book entitled *Funding Evil: How Terrorism is Financed and How to Stop It*, which alleged that Mahfouz financed al-Qaida in the years leading up to 9/11, a claim that Mahfouz strenuously denied. An English court agreed to hear the case even though the book had not been published in the UK, because some copies were bought online in the UK. Ehrenfeld did not appear in the UK to defend the claim, and Mahfouz was awarded substantial damages.

Ehrenfeld then sued Mahfouz in New York to obtain a declaration that the judgment would not be enforced in the US because her book was not defamatory under US law. That action was dismissed and, in response to this

judgement, the New York State Legislature passed the Libel Terrorism Protection Act. The link between libel terrorism and libel tourism has played a large part in convincing politicians to adopt the New York law into Federal Law. The article below continues the story from the perspective of across the Atlantic.

These issues of jurisdiction have a significance beyond libel law. As e-book and digital delivery finally begin to

## 2. The US perspective

The US is also a nice place for tourists to visit – except for those who have come with freshly-minted UK libel judgments, and are asking US courts to enforce those judgments. They will go home disappointed and un-enriched. In fact, a counter-offensive against UK libel tourism is being launched by the US Congress and various state legislatures.

To begin with, there is no automatic enforcement of any UK judgment in the United States. Most states apply a version of something called the Uniform Foreign Money-Judgments Recognition Act in deciding whether to recognize and enforce the judgments of foreign courts. The Act expressly provides that state courts may refuse to enforce judgments where “the cause of action on which the judgment is based is repugnant to the public policy of this state.”

The libel judgments of UK courts are on a particularly shaky footing in the US. Beginning with the US Supreme Court’s *New York Times v. Sullivan* decision in 1964, US courts have significantly modified state libel rules in order to protect the freedom of speech guaranteed by the First Amendment to the United States Constitution. As a constitutional matter, US libel claimants must prove that a challenged statement is false, whereas a defendant in the UK bears the burden of proving the truth of the statement. UK law imposes essentially a strict liability standard, whereas US claimants must show that the defendant published with fault (at a minimum, negligence).

If the claimant is a “public figure”, he must show much more: that the defendant published with knowledge or reckless disregard of the statement’s falsity. Where the

take off the ability to publish on a truly global basis is closer to reality for many publishers. The tremendous opportunity this provides is matched with some of the challenges that local legal and regulatory restrictions can throw up. Not just in London, but in any city in any territory, where the business of advertising, trading, selling, taxing and delivering books (in whatever form) may be very different to that in the home state of the publisher.

challenged statement is about a genuine matter of public interest, some states require that even a “private” claimant show that the defendant was grossly negligent or violated accepted standards of journalism.

US courts are aware that UK libel law falls well short of US constitutional standards, and for a number of years have refused to enforce UK libel judgments, finding them repugnant to state public policy. The Mahfouz case, summarized in the article above, has shifted the focus from the courtroom to the legislature. As Duncan and Alan note, Rachel Ehrenfeld sued to have a New York federal court declare that Kahlid bin Mahfouz’s UK libel judgment was unenforceable, but her claims foundered on the limited scope of New York’s “long arm” statute, which governs jurisdiction over non-residents. Mahfouz’s contacts with New York were found to be so attenuated as to place him outside of long arm jurisdiction.

The New York legislature acted promptly to stretch the “long arm”: it enacted the New York Libel Terrorism Protection Act. A New York resident may now obtain jurisdiction over any foreign libel claimant for an action declaring that the claimant’s foreign judgment against the resident is unenforceable in New York. The law also expressly bars enforcement in New York of foreign libel judgments unless the rendering country provides at least as much protection for freedom of speech as does the First Amendment.

At least five other states have enacted or will soon enact similar statutes. However, it is most likely that Congressional action will supersede these state laws.

Currently, Congress is considering the Free Speech Protection Act of 2009, which has already passed the House by a large margin and is now before the Senate. The new bill will allow US citizens and businesses, who have been sued for libel abroad on the basis of any writing that was primarily disseminated in the US, to bring a United States action if the speech would not be defamation under US law. The US court could order non-enforcement of the foreign libel judgment, damages against the claimant and what might be called the “nuclear option”. If the US court finds that the foreign libel claimant was engaged in a “scheme to suppress First Amendment rights” by discouraging publishers not to publish the US person’s works, it can award treble damages against the claimant. The latter provision was

included with full knowledge that UK courts will not enforce US awards that exceed actual damages.

While the Senate is currently occupied with even larger matters (national health care), the Free Speech Protection Act is likely to become law within the next year. It will be interesting to see the response. Will UK courts modify their loose standards of jurisdiction to appease an irate US Congress? Will libel tourists think twice about suing in the UK when they run the risk of a US treble damages award? Or will there be a stalemate: judicial dockets clogged with UK libel judgments that US courts will not enforce and US treble damages awards that the UK and the home countries of libel tourists will not enforce? Only time will tell. ■

# Key specialists

Should you wish to receive more information on these topics, please contact the following partners from our Intellectual Property and Technology Group:

Amsterdam	Joris Willems	+31 20 541 9992	joris.willems@dlapiper.com
Brussels	Patrick Van Eecke	+32 2 500 16 30	patrick.vaneecke@dlapiper.com
Bucharest	Marian Dinu	+40 21 202 3020	marian.dinu@dlapiper.com
Dubai	Matt Glynn Lenka Glynn	+971 4 438 6282 +971 4 438 6285	matt.glynn@dlapiper.com lenka.glynn@dlapiper.com
Hong Kong	Gigi Cheah	+852 2103 0621	gigi.cheah@dlapiper.com
London	Duncan Calow	+44 20 7796 6473	duncan.calow@dlapiper.com
Madrid	Diego Ramos	+34 91 319 1212	diego.ramos@dlapiper.com
Milan	Giorgio Olivi	+39 2 806181	giorgio.olivi@dlapiper.com
Munich	Thomas Jansen	+49 89 23 23 72 0	thomas.jansen@dlapiper.com
Palo Alto	Mark Radcliffe	+1 650 833 2266	mark.radcliffe@dlapiper.com
Paris	Carol Umhoefer	+33 1 40 15 24 00	carol.umhoefer@dlapiper.com
Prague	Peter Valert	+420 222 817 366	peter.valert@dlapiper.com
Rome	Italo de Feo	+39 6 68 88 01	italo.defeo@dlapiper.com
Sofia	Peter Valert	+420 222 817 366	peter.valert@dlapiper.com
Stockholm	Jan Bryme	+46 8 701 78 83	jan.bryme@dianordic.se
Tokyo	Lawrence Carter	+81 03 4550 2811	lawrence.carter@dlapiper.com
Vienna	Wolfgang Freund	+43 1 531 78 1401	wolfgang.freund@dlapiper.com
Warsaw	Marlena Wach	+48 22 540 74 13	marlena.wach@dlapiper.com
Washington DC	Jim Halpert Heidi Salow	+1 202 799 4441 +1 202 799 4444	jim.halpert@dlapiper.com heidi.salow@dlapiper.com

DLA Piper UK LLP (1) and DLA Piper Scotland LLP (2) are part of DLA Piper, an international legal practice, the members of which are separate and distinct legal entities. For further information please refer to [www.dlapiper.com/structure](http://www.dlapiper.com/structure). A list of offices can be found at [www.dlapiper.com](http://www.dlapiper.com). Regulated by (1) the Solicitors Regulation Authority, (2) the Law Society of Scotland. Belgium switchboard +32 (0)2 500 1500. Copyright © 2009 DLA Piper. All rights reserved.

You are receiving this communication because you are a valued client, former client or friend of DLA Piper. The information contained in this newsletter is for informational purposes only, and should not be construed as legal advice on any matter.