Volume 5, Issue 7, December 2014

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

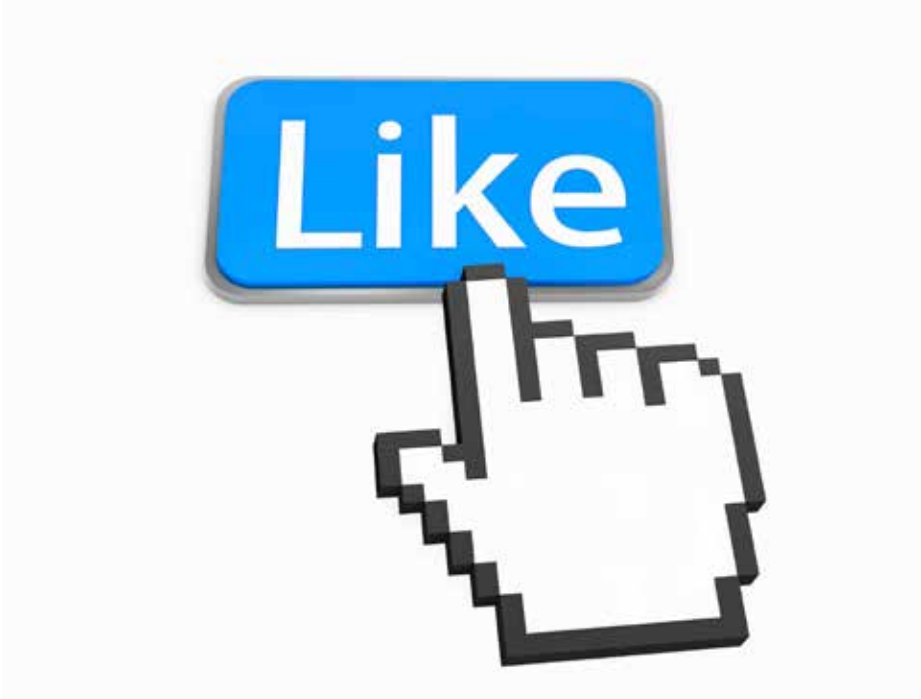
Patrick Bernhardt
Chris Coulter
John F. Delaney
Anelia V. Delcheva
Christine E. Lyon
Julie O'Neill
Anthony M. Ramirez
Karin Retzer
Aaron P. Rubin
Cara Ann Marr Rydbeck
Mercedes Samavi
Sarah Wells

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER



Welcome to the newest issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media. In this edition—which we have dubbed the "like" issue—we look at several topics surrounding the proverbial online thumbs up, including the emerging legal status of Facebook likes and similar social media constructs; Facebook's recent prohibition of the popular business practice of offering discounts, exclusive content and other incentives in exchange for liking a company's Facebook page; and Facebook's crackdown on the practice of buying phony likes. We realize though that likes aren't everything, so we also explore the legal framework for moving personal data to the cloud; we examine clickwraps vs. browsewraps in relation to the implementation and enforcement of online terms of use; we discuss the new California privacy law revisions impacting website and mobile app operators directing their services to minors; we take a look at the new infringement exceptions in the United Kingdom; and we highlight a recent decision in the UK granting a website-blocking order against certain ISPs in a case involving counterfeit goods.

All this—plus an infographic about—what else?—Facebook likes.

WHAT'S IN A LIKE?

By Aaron Rubin and Cara Ann Marr Rydbeck

In the pre-Facebook era, the word "like" was primarily a verb (and an interjection sprinkled throughout valley girls' conversations). Although you could have likes and dislikes in the sense of preferences, you could not give someone a like, claim to own a like or assert legal rights in likes. Today, however, you can do all of these things and more with Facebook likes and similar constructs on other social media platforms, such as followers, fans and connections. This article explores the emerging legal status of likes and similar social media constructs as the issue has arisen in a number of recent cases.

LIKES AS PROTECTED SPEECH

One of the early cases to delve into the legal status of likes was *Bland v. Roberts*, which addressed the issue of whether a Facebook like constitutes protected speech for purposes of the First Amendment. In *Bland*, five former employees of the Hampton Sheriff's Office brought a lawsuit against Sheriff Roberts, alleging that he violated their First Amendment rights to freedom of speech and freedom of association when he fired them, allegedly for having supported an opposing candidate in the local election. In particular, two of the plaintiffs had "liked" the opposing candidate's Facebook page.

Although—as we discussed previously—the district court held that merely liking a Facebook page was insufficient speech to merit constitutional protection, on appeal the Fourth Circuit reversed and held that liking a Facebook page does constitute protected speech. The Fourth Circuit looked at what it means to like a Facebook page and concluded: "On the most basic level, clicking on the 'like' button literally causes to be published the statement that the User 'likes' something, which is itself a substantive statement." The Fourth Circuit also found that liking a Facebook page is symbolic expression because "[t]he distribution of the universally understood 'thumbs up' symbol in association with [the] campaign page, like the actual text that liking the page produced, conveyed that [the plaintiff] supported [the opposing candidate's] candidacy." The court analogized liking the opposing candidate's Facebook page as the "Internet equivalent of displaying a political sign in one's front yard, which the Supreme Court has held is substantive speech."

Perhaps most interestingly from a business perspective, various cases have explored the question of ownership of a like—and similar concepts, such as a Twitter follower or LinkedIn connection.

LIKES AS PROPERTY

Perhaps most interestingly from a business perspective, various cases have explored the question of ownership of a like—and similar concepts, such as a Twitter follower or LinkedIn connection. In *Mattocks v. Black Entertainment Television LLC*, the plaintiff Mattocks created an unofficial Facebook fan page focused on the television series *The Game*, which at the time was broadcast on the CW Network; BET later acquired the rights to *The Game* from the CW Network. BET eventually hired Mattocks to perform part-time work for BET, including paying her to manage the unofficial fan page. During the course of that relationship, BET provided Mattocks with BET logos and exclusive content to display on the fan page, and both Mattocks and BET employees posted material on the fan page. While Mattocks worked for BET, the fan page's likes grew from around two million to more than six million.

Mattocks and BET began discussions about Mattocks' potential full-time employment at BET but, at some point during these discussions, Mattocks demoted BET's administrative access to the fan page. After losing full access to the fan page, BET asked Facebook to "migrate" fans of the page to another official Facebook fan page created by BET. Facebook granted BET's request and migrated the likes to the other BET-sponsored page. Facebook also shut down Mattocks' fan page. Mattocks then sued BET in the Southern District of Florida, alleging, among other things, that BET converted a business interest she had in the fan page by migrating the likes. Mattocks argued that the page's "significant number of likes" provided her with business opportunities based on companies paying to have visitors redirected to their sites from the page. BET moved for summary judgment.

The district court granted BET's motion for summary judgment on Mattocks' conversion claim, holding that Mattocks failed to establish that she owned a property interest in the likes. The court explained that "liking" a Facebook page simply means that the user is expressing his or her enjoyment or approval of the content, and that the user is always free to revoke the like by clicking an unlike button. Citing *Bland* (discussed above), the court stated that "if anyone can be deemed to own the 'likes' on a [Facebook page], it is the individual users responsible for them." Given the tenuous relationship between the creator of the Facebook page and the likes of that page, the court held that likes cannot be converted in the same manner as goodwill or other intangible business interests.

In *PhoneDog v. Kravitz*, the district court for the Northern District of California denied defendant Kravitz's motion to dismiss plaintiff PhoneDog's claims for, among other things,

Facebook users generate 4.5 billion likes per day[1]

WHAT DO WE LIKE?

- Facebook posts with photos get 53% more likes than text-based posts.[2]
- Facebook posts with emoticons get 57% more likes than posts without emoticons.[2]
- 87.7 million users like the Facebook page for Shakira, the most-liked person on Facebook.[3 & 4]
- 80.9 million users like the Facebook page for Coca-Cola, the most-liked product page on Facebook. [3 & 5]
- 71.7 million users like the Facebook page for The Simpsons, the most-liked TV show page on Facebook. [3 & 6]

HOW OFTEN DO WE LIKE?

- 44% of Facebook users like their friends' content once a day.[7]
- 29% of Facebook users like their friends' content several times a day.[7]

SOURCES

1. https://zephoria.com/social-media/top-15-valuable-facebook-statistics/
2. http://www.fastcompany.com/3022301/work-smart/7-powerful-facebook-statistics-you-should-know-about
3. http://www.insidefacebook.com/2014/09/02/top-25-facebook-pages-september-2014-facebook-for-every-phone-nearing-500m-likes/
4. http://pagedatapro.com/pages/facebook/shakira/5027904559
5. http://pagedatapro.com/pages/facebook/coca-cola/40796308305
6. http://pagedatapro.com/pages/facebook/the-simpsons/29534858696
7. http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook/

conversion of the Twitter account "@PhoneDog_Noah." PhoneDog, a mobile news and reviews website, employed Kravitz as a product reviewer and video blogger. Kravitz maintained the Twitter account "@PhoneDog_Noah," which he used to post product reviews, eventually accumulating 17,000 Twitter followers. At the end of Kravitz's employment, PhoneDog requested that Kravitz relinquish use of the Twitter account. Kravitz refused, changed the Twitter handle to "@noahkravitz" and continued to use the account.

PhoneDog claimed an "intangible property interest" in the Twitter account's followers, which PhoneDog compared to a business customer list. Kravitz disputed PhoneDog's ownership interest in either the Twitter account or its followers, based on Twitter's terms of service, which state that Twitter accounts belong to Twitter and not to Twitter users such as PhoneDog. Kravitz also argued that Twitter followers are "human beings who have the discretion to subscribe and/or unsubscribe" to the account and are not PhoneDog's property. The court held that there was insufficient evidence to determine whether or not PhoneDog had any property interest in the Twitter followers, and denied Kravitz's motion to dismiss. PhoneDog and Kravitz subsequently settled the dispute so we will never know how the court would have ruled on this issue, but the court's refusal to dismiss PhoneDog's ownership claims may indicate that, at least in some circumstances, Twitter followers may constitute property.

The district court in the Eastern District of Pennsylvania looked at a similar issue involving ownership of a LinkedIn account in *Eagle v. Morgan*. Plaintiff Linda Eagle established a LinkedIn account using the email address of Edcomm, the banking education company that she co-founded with Clifford Brody. As CEO of Edcomm, Brody embraced LinkedIn as a sales and marketing tool for the Edcomm business. Although Edcomm did not require employees to maintain or subsidize the maintenance of LinkedIn accounts, it did develop policies with respect to employee use of such accounts.

When Eagle (and Brody) were involuntarily terminated after Edcomm's acquisition by another company, Edcomm employees accessed Eagle's LinkedIn account (using the password she had disclosed to certain employees) and changed its password, effectively locking Eagle out of the account. For more than two weeks, Edcomm had full control of the account. During that time, it replaced the account information regarding name, picture, education and experience with information about Sandi Morgan, the newly appointed Interim CEO of Edcomm. As a result, during this time period, an individual conducting a search on either Google or LinkedIn for Eagle (by typing in "Linda Eagle") would be directed to a URL for a web page showing Sandi Morgan's name, profile and affiliation with Edcomm. LinkedIn subsequently intervened and restored Eagle's access to the account.

Eagle filed suit against Edcomm, alleging compensatory damages of between $248,000 and $500,000. Eagle used a

damages formula that attributed her total past revenue to business generated by the number of connections associated with the LinkedIn account in order to establish a dollar value per LinkedIn connection, and then used that value to calculate her damages for the period of time that she was unable to access the LinkedIn account. The court found for Eagle on a number of her claims—including claims for unauthorized use of name under a Pennsylvania statute, invasion of privacy and misappropriation of publicity—but the court ultimately held that Eagle's damages request was not supported by sufficient evidence, citing, for example, her failure to connect her past sales to use of LinkedIn.

Although Eagle's claim was unsuccessful, the use of LinkedIn connections to support her damages theory demonstrates the potential monetary value of these connections and the importance for companies to be clear with their employees in delineating ownership of social media accounts and associated likes, followers, fans and connections.

LIKES AS CONCERTED ACTIVITY

There have been a number of National Labor Relations Board (NLRB) decisions that examined whether an employee's statements on social media constitute "concerted activity"—activity by two or more employees that provides mutual aid or protection regarding terms or conditions of employment—for purposes of the National Labor Relations Act (NLRA).

In Pier Sixty LLC, the administrative law judge decided that a Facebook posting made by an employee about his supervisor constituted protected concerted activity under the NLRA, despite being sprinkled with obscenities. The decision held that the posting constituted part of an ongoing sequence of events related to the employees' dissatisfaction with the manner in which they were treated by their managers. The administrative law judge specifically mentioned that because the employee was friends on Facebook with several other employees, he could anticipate that those other employees, who were also concerned with the supervisor's demeaning treatment, would see the posting (at the time, the employee had set his Facebook page so that it could only be viewed by his friends).

Similarly, in Richmond District Neighborhood Center, a Facebook conversation between two employees was found to be concerted activity under the NLRA because it involved the employees voicing their disagreement with the management's running of the center. However, the administrative law judge ultimately concluded that the activity was not protected under the NLRA because it "jeopardized the program's funding and the safety of the youth it serves" and demonstrated that the two employees were "unfit for further service."

Although these two NLRB cases involved postings and conversations on Facebook rather than just likes, it would not be a huge leap for a future NLRB case to hold that a Facebook like constitutes concerted activity in certain circumstances, particularly in light of the Fourth Circuit's decision in *Bland*, discussed above.

• • • • •

As the legal status of likes, followers, fans and connections continues to develop, we are likely to see more cases in which courts and litigants struggle with the question of whether and in what circumstances these social media constructs constitute valuable business assets and legitimate forms of speech and communication. At least in the legal sense, "like" has come a long way from the valley girl lexicon—like, a really long way.

R.I.P.: The Facebook "Like" Gate

By Anthony M. Ramirez

Do you still "like" me? Companies with Facebook pages will find themselves asking that question of their followers over the next few weeks, as Facebook brings an end to the popular practice of offering discounts, exclusive content and other incentives in exchange for liking a page.

The like gate disappeared almost as quickly as it had become widespread. Following a 90-day grace period, a new Facebook rule took effect on November 5, 2014, identifying three—and only three—specific actions on Facebook that users could be incentivized to perform.

Facebook had previously facilitated this exchange by allowing page operators to reveal certain content only to users who had liked the page. This practice was known as "like gating." The exclusive content might have included coupon codes, contest entry forms, voting buttons for polls and other content that would create an incentive for the user to like the page. Even altruistic incentives have been offered, such as promises by brands to donate a dollar to charity for each like that their page receives.

Like gating became a popular—and successful—way for companies to build followers for their Facebook pages. We won't know exactly how many of the 4.5 billion likes per day received on Facebook were due to like gating, but the number was certainly significant.

The like gate disappeared last month almost as quickly as it had become widespread. Following a 90-day grace period, a new Facebook rule took effect on November 5, 2014, identifying three—and only three—specific actions on Facebook that users could be incentivized to perform.

Companies quickly realized that liking a page was conspicuously absent from that list of actions. (It remains permissible to provide incentives for users to log into a Facebook app, to enter a promotion on a Facebook app's page, and to check into a place.)

In a blog post announcing this change, Facebook made clear that companies "must not incentivize people to use social plugins or to like a page." Facebook also provided its behind-the-scenes reasoning on the change. Facebook believes that eliminating the practice of like gating will help "ensure quality connections and help businesses reach the people who matter to them" rather than building relationships on Facebook that are based on "artificial incentives."

Companies will undoubtedly find ways to continue building their presences on Facebook without using the like gate. Indeed, many marketers had already been advising that like gating was quickly becoming an outdated practice, and that the followers generated by like gating were less valuable than followers generated organically.

The next time you log into Facebook, you may find your favorite brand asking you to engage with the brand in a more substantial way, such as by submitting user-generated content, instead of simply liking its page. Known as "action gating," this alternative practice is already being touted by marketers as a way to build a more valuable online fan base through more active types of engagement.

The like gate is dead. Long live the action gate.

FACEBOOK DISLIKES FAKE LIKES

By John Delaney

Money may not be able to buy happiness, but it can buy phony Facebook "likes."

And those can go a long way toward making a small business owner's dreams come true, right?

Wrong, explains Facebook site integrity engineer Matt Jones in a recent post on the company's official blog.

Phony likes don't help companies to reach their target audiences on Facebook because, for one thing, the creators of phony likes—which usually originate from fake Facebook accounts or real ones that have been hacked into—aren't actual paying customers with whom the business would benefit from communicating.

Businesses that purchase fake likes "won't achieve results and could end up doing less business on Facebook if the people they're connected to aren't real," Jones observes.

Phony likes don't help companies to reach their target audiences on Facebook because, for one thing, the creators of phony likes—which usually originate from fake Facebook accounts or real ones that have been hacked into—aren't actual paying customers with whom the business would benefit from communicating, digital marketing gurus explain.

Nor do phony likes represent people who are likely to be Facebook friends with consumers looking for peer recommendations.

Further, fake likes won't increase the likelihood that the business purchasing them will reach a relevant wider audience because, according to Jones, the Facebook algorithm that decides when and where to deliver a page's legitimate ads and content takes page engagement rates into account, and "the people involved [in creating a fake like] are unlikely to engage with a page after liking it initially."

As one digital marketing blogger notes, "[Q]uantity [is] not the metric that [is] important with Facebook marketing; it's all about the quality. Having 10,000 fans in India is great, but they're not going to buy anything or visit you if you're a furniture store in Sydney, Australia."

And so, for these reasons, and for the sake of maintaining its own advertising-dependent business model, Facebook is doing all it can to rid the social network of phony likes, reports Jones. The company's efforts to achieve this end include automated measures such as algorithms that block spam and help Facebook to identify fraudulent activity. The company also asks for verification from accounts with particularly high like activity.

Indeed, Facebook's recent ban on the practice of "like" gating—discussed elsewhere in this issue—appears to be part of this same initiative to ensure the legitimacy—and marketing value—of each individual like.

There is one group of businesses for whom bogus likes make economic sense: Those that profit from selling such likes. Pssst—wanna buy a like? For $480, you can reportly purchase 10,000 likes, while $1,200 gets you 50,000 new likes. It's big business: a 2013 study estimated that fake Facebook activities generate $200 million a year. But Facebook is fighting back.

Jones's Facebook blog post highlights the nearly $2 billion in legal judgments that the social media platform obtained by filing lawsuits against spammers. The most publicized of those suits concern more traditional spamming—the gaining of unauthorized access to Facebook user accounts for the purpose

of sending unsolicited commercial electronic messages. But Facebook has filed at least one suit against a seller of phony likes, and, based on Jones's statements, one can expect Facebook to commence more such suits in the future.

And while Facebook isn't likely to see much money from these lawsuits—the defendants often file for bankruptcy or simply disappear—the resulting judgments are likely to deter parties from selling phony likes.

As we explore elsewhere in this issue, the Facebook like has now achieved legal status—as property, as protected speech under the First Amendment and as protected "concerted activity" under the National Labor Relations Act. So it's not surprising that, with the growing business and legal importance of the like, we're seeing a greater effort on Facebook's part to ensure the integrity of the like.

And, if it is to have integrity, a like needs to be earned, not bought.

PRIVACY IN THE CLOUD: A LEGAL FRAMEWORK FOR MOVING PERSONAL DATA TO THE CLOUD

By Christine E. Lyon and Karin Retzer

For many companies, the main question about cloud computing is no longer whether to move their data to the "cloud," but how they can accomplish this transition. Cloud (or Internet-based on-demand) computing involves a shift away from reliance on a company's own local computing resources, in favor of greater reliance on shared servers and data centers. Well-known examples of cloud computing services include Google Apps, Salesforce.com, and Amazon Web Services. In principle, a company also may maintain its own internal "private cloud" without using a third-party provider. Since many companies choose to use third-party cloud providers, however, this article will focus on that cloud computing model.

The flexibility and easy flow of data that characterize the cloud can raise challenging issues related to protection of data in the cloud. A company's legal obligations and risks will be shaped by the nature of the data to be moved to the cloud, whether the data involve personal information, trade secret information, customer data or other competitively sensitive information.

Cloud computing offerings range from the provision of IT infrastructure alone (servers, storage and bandwidth) to the provision of complete software-enabled solutions. Cloud computing can offer significant advantages in cost, efficiency and accessibility of data. The pooling and harnessing of processing power provides companies with flexible and cost-efficient IT systems. At the same time, however, cloud computing arrangements tend to reduce a company's direct control over the location, transfer and handling of its data.

The flexibility and easy flow of data that characterize the cloud can raise challenging issues related to protection of data in the cloud. A company's legal obligations and risks will be shaped by the nature of the data to be moved to the cloud, whether the data involve personal information, trade secret information, customer data or other competitively sensitive information. This article describes the special legal considerations that apply when moving personal information to the cloud. It also offers a framework to help companies navigate these issues to arrive at a solution that meets their own legal and business needs.

DETERMINE THE CATEGORIES OF PERSONAL INFORMATION TO BE MOVED TO THE CLOUD

As a general principle, personal information includes any information that identifies or can be associated with a specific individual. Some types of personal information involve much greater legal and business risks than other types of personal information. For example, a database containing health information will involve greater risks than a database containing names and business contact information of prospective business leads. Also, financial regulators in many countries require specific security standards for financial information. Accordingly, a cloud computing service that may be sufficient for the business lead data may fail to provide the legally required level of protection for health, financial or other sensitive types of information.

A company will want to develop a strategy that provides sufficient protection to the most sensitive personal information to be transmitted to the cloud. In some cases, a company may elect to maintain certain types of personal information internally, in order to take advantage of more cost-efficient cloud computing services for its less-sensitive data.

IDENTIFY APPLICABLE LAWS AFFECTING YOUR OUTSOURCING OF PERSONAL INFORMATION

Cloud computing, by its nature, can implicate a variety of laws, including privacy laws, data security and breach

notification laws, and laws limiting cross-border transfers of personal information.

(a) Privacy Laws

Companies operating in the United States will need to consider whether they are subject to sector-specific privacy laws or regulations, such as the Gramm-Leach-Bliley Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA). Such laws impose detailed privacy and data security obligations, and may require more specialized cloud-based offerings.

Europe-based companies, as well as companies working with providers in or with infrastructure in Europe, will need to account for the broad-reaching requirements under local omnibus data protection laws that protect all personal information, even basic details like business contact information. These requirements can include notifying employees, customers or other individuals about the outsourcing and processing of their data; obligations to consult with works councils before outsourcing employee data; and registering with local data protection authorities. Similar requirements arise under data protection laws of many other countries, including countries throughout Europe, Asia, the Middle East and the Americas.

(b) Data Security Requirements

Even if a company is not subject to these types of privacy laws, it will want to ensure safeguards for personal information covered by data security and breach notification laws. In the U.S., these laws tend to focus on personal information such as social security numbers, driver's license numbers and credit or debit card or financial account numbers. One of the key safeguards is encryption because many (although not all) of the U.S. state breach notification laws provide an exception for encrypted data.

In contrast, many other countries require protection of all personal information, and do not necessarily provide an exception for encrypted data. Consequently, companies operating outside of the U.S. may have broader-reaching obligations to protect all personal information. While data protection obligations vary significantly from law to law, both U.S. and international privacy laws commonly require the following types of safeguards:

i. Conducting appropriate due diligence on providers;

ii. Restricting access, use, and disclosure of personal information;

iii. Establishing technical, organizational, and administrative safeguards;

iv. Executing legally sufficient contracts with providers; and

v. Notifying affected individuals (and potentially regulators) of a security breach compromising personal information.

The topic of data security in the cloud has received significant industry attention. Industry groups, such as the Cloud Security Alliance (CSA), have suggested voluntary guidelines for improving data security in the cloud. For example, please refer to the CSA's Security Guidelines for Critical Areas of Focus for Cloud Computing, available at https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/. In Europe, the Cloud Select Industry Group (CSIG), an industry group sponsored by the European Commission, recently issued the Cloud Service Level Agreement Standardization Guidelines, available at http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines. The Guidelines recommend contractual stipulations covering (1) business continuity, disaster recovery and data loss prevention controls; (2) authentication/authorization controls, including access provision/revocation, and access storage protection; (3) encryption controls; (4) security incident management and reporting controls and metrics; (5) logging and monitoring parameters and log retention periods; (6) auditing and security certification; (7) vulnerability management metrics; and (8) security governance metrics. Providers also may choose to be certified under standards such as ISO 27001, although such certifications may not address all applicable legal requirements.

(c) Restrictions on Cross-Border Data Transfers

A number of countries—e.g., all the European Economic Area (EEA) Member States and certain neighboring countries (including Albania, the Channel Islands, Croatia, the Faroe Islands, the Isle of Man, Macedonia, Russia and Switzerland), as well as countries in North Africa (e.g., Morocco), the Middle East (e.g., Israel), Latin America (e.g., Argentina and Uruguay), and Asia (e.g., South Korea)—restrict the transfer or sharing of personal information beyond their borders. These restrictions can present significant challenges for multinational companies seeking to move their data to the cloud. Recognizing these challenges, some providers are starting to offer geographic-specific clouds, in which the data are maintained within a given country or jurisdiction. Some U.S. providers have also certified to the U.S.-European Union Safe Harbor program, in order to accommodate EU-based customers. As the Safe Harbor only permits transfers from the EU to the U.S., however, it is not a global solution. Accordingly, a company should assess carefully whether the options offered by a provider are sufficient to meet the company's own legal obligations in the countries where it operates.

To complicate matters, international data protection authorities, particularly in the EEA, have expressed concerns about use of the cloud model for personal information. The Working

Party 29 (WP29), the assembly of EEA data protection authorities, and many other local EEA authorities have issued guidance about cloud computing, covering purpose and transfer restrictions, notification requirements, mandatory security requirements, and the content of the contract to be concluded with cloud providers. This guidance includes the WP29 Opinion 05/2012 on Cloud Computing, which is discussed further below. The draft Data Protection regulation currently discussed among the EEA Member States reflects such guidance and should be accounted for prior to engaging cloud providers.

REVIEW CONTRACTUAL OBLIGATIONS AFFECTING YOUR OUTSOURCING OF PERSONAL INFORMATION

If your company is seeking to outsource to a cloud provider applications that involve third-party data, such as personal information maintained on behalf of customers or business partners, it is important to consider any limitations imposed by contracts with those third parties. Such agreements might require third-party consent to the outsourcing or subcontracting of data processing activities, or may require your company to impose specific contractual obligations on the new provider or subcontractor.

SELECT AN APPROPRIATE CLOUD COMPUTING SOLUTION

Cloud services tend to be offered on a take-it-or-leave-it basis, with little opportunity to negotiate additional contractual protections or customized terms of service. As a result, companies may find themselves unable to negotiate the types of privacy and data security protections that they typically include in contracts with other service providers. Companies will need to evaluate whether the contract fulfills their applicable legal and contractual obligations, as discussed above. Beyond that, companies will want to evaluate the practical level of risk to their data, and what steps they might take to reduce those risks.

(a) Public vs. Private Cloud

Broadly speaking, a private cloud maintains the data on equipment that is owned, leased or otherwise controlled by the provider. Private cloud models can be compared with many other well-established forms of IT outsourcing and do not tend to raise the same level of concerns as a public cloud model.

A public cloud model disperses data more broadly across computers and networks of unrelated third parties, which might include business competitors or individual consumers. While offering maximum flexibility and expansion capabilities, the public cloud model raises heightened concerns about the inability to know who holds your company's data, the lack of oversight over those parties and the absence of standardized data security practices on the hosting equipment. Given these challenges, companies outsourcing personal information will want to understand whether the proposed service involves a private or public cloud, as well as evaluate what contractual commitments the provider is willing to make about data security.

(b) Securing Data Before Transmission to the Cloud

Companies also may be able to take measures themselves to protect personal information before it is transmitted to the cloud. Some provider agreements instruct or require customers to encrypt their data before uploading the data to the cloud, for example. If it is feasible to encrypt the data prior to transmission to the provider, this may provide substantial additional protections, as long as the encryption keys are not available to the provider.

It is also important to account for applicable security requirements. To this effect, several countries in Europe have very specific statutory requirements for security measures, and some regulators have issued detailed security standards for cloud computing providers. Pursuant to the WP29 Opinion 05/2012, all contracts should include security measures in accordance with EU data protection laws, including requirements for cloud providers on technical and organizational security measures, access controls, disclosure of data to third parties, cooperation with the cloud client, details on cross-border transfer of data, logging and auditing processing. The recent guidelines from the CSIG recommend the inclusion of the following provisions in processing agreements: (1) standards or certification mechanisms the cloud service provider complies with; (2) precise description of purposes of processing; (3) clear provisions regarding retention and erasure of data; (4) reference to instances of disclosure of personal data to law enforcement and notification to the customer of such disclosures; (5) a full list of subcontractors involved in the processing and inclusion of a right of the customer to object to changes to the list, with special attention to requirements for processing of special or sensitive data; (6) description of data breach policies implemented by the cloud service provider including relevant documentation suitable to demonstrate compliance with legal requirements; (7) clear description of geographical location where personal data is stored or processed, for purposes of implementing appropriate cross-border transfer mechanisms; and (8) time period necessary for a cloud service provider to respond to access, rectification, erasure, blocking or objection requests by data subjects.

(c) Contract Issues

In the majority of cloud computing services, the client is the data controller and the cloud provider is the data processor. However, in certain scenarios—in particular Platform as a Service (PaaS) and Software as a Service (SaaS) in public computing models—the client and the cloud provider may be joint controllers. Under EU guidance, the responsibilities of joint controllers must be very clearly set out in the

contract to avoid any "dilution" of legal responsibility.

The contract with the cloud services provider needs to set out clearly the roles and responsibilities of the parties. Unlike many outsourcing arrangements, cloud service contracts usually do not distinguish between personal information and other types of data. These contracts may still include at least basic data protection concepts, even if they are not expressly identified as such. At a minimum, companies will want to look for provisions preventing the provider from using the information for its own purposes, restricting the provider from sharing the information except in narrowly specified cases, and confirming appropriate data security and breach notification measures. Various European data protection authorities have underscored that access to cloud data by public authorities must comply with national data protection law and that the contract should require notification of any such requests unless prohibited under criminal law and should prohibit any non-mandatory sharing. Given the difficulty of negotiating special arrangements with cloud providers, it is important to select a cloud offering that is appropriately tailored to the nature of the data and the related legal obligations. It is likely that as cloud computing matures, more offerings tailored to specific business requirements, including compliance with privacy and similar laws, will be made available to companies.

CONCLUSION

While cloud computing can substantially improve the efficiency of IT solutions, particularly for small- and medium-sized businesses, the specific offerings need to be examined closely. There is no "one-size-fits-all" solution to cloud computing, especially for companies operating in highly regulated sectors or internationally. By understanding their legal compliance obligations, companies can make informed decisions in selecting cloud computing services or suites of services that best meet their needs.

CLICK IT UP: IMPLEMENTING AND ENFORCING ONLINE TERMS OF USE

By Aaron Rubin and Anelia V. Delcheva

Operators of social media platforms and other websites must manage a large number of risks arising from their interactions with users. In an effort to maintain a degree of predictability and mitigate some of those risks, website operators routinely present users with terms of use or terms of service ("Website Terms") that purport to govern access to and use of the relevant website and include provisions designed to protect the website operators, such as disclaimers, limitations of liability and favorable dispute resolution provisions. But are such Website Terms enforceable against users and do they actually provide the protection that website operators seek? The answer may well depend on how the Website Terms are implemented.

In determining whether Website Terms are enforceable against users, U.S courts generally focus on whether users had notice of the terms and actually agreed to be bound by them.

CLICKWRAP VS. BROWSEWRAP

Website Terms typically come in two flavors: "clickwrap" terms, where users are required to accept by taking some affirmative action such as checking a box or clicking an "I accept" button before using the website, and "browsewrap" terms that are provided to users through a link—often, but not always, at the bottom of the page—and purport to bind users even without any affirmative manifestation of acceptance. In determining whether Website Terms are enforceable against users, U.S. courts generallly focus on whether users had notice of the terms and actually agreed to be bound by them. Not surprisingly, therefore, courts tend to look more favorably on clickwrap implementations as compared to browsewrap terms.

For example, in *Fteja v. Facebook, Inc.* (S.D.N.Y. 2012), the plaintiff claimed that Facebook disabled his Facebook account without justification and for discriminatory reasons, causing emotional distress and harming his reputation. Facebook moved to transfer the case to federal court in Northern California based on the forum selection clause in the Facebook terms of use, but the plaintiff claimed that he had never agreed to the terms of use. The court concluded that the plaintiff was bound by the Facebook terms, however, because he had checked a box indicating his acceptance when he registered for Facebook.

In contrast, Barnes & Noble had less luck enforcing its terms of use in *Nguyen v. Barnes & Noble, Inc.* (9th Cir. Aug. 18, 2014). In Nguyen, the plaintiff ordered a tablet from Barnes & Noble at a discounted price but Barnes & Noble canceled his order. The plaintiff sued and Barnes & Noble moved to compel arbitration based on an arbitration clause included in its website's browsewrap terms of use. The court held that Barnes & Noble's terms could not bind the plaintiff, despite being presented through a "conspicuous" link during the checkout process, because Barnes & Noble did not prompt users to affirmatively assent to the terms.

EVIDENTIARY ISSUES

In general, then, clickwrap Website Terms are more likely to be enforceable than are browsewrap implementations. But even if a website operator implements its Website Terms through a clickwrap, how can the operator prove that an individual user actually accepted

the terms in a particular case? That issue arose in *Moretti v. Hertz Corporation* (N.D. Cal. Apr. 11, 2014). In *Moretti*, the plaintiff had booked a car rental on the Hotwire website and alleged that he was overcharged. The defendants invoked a forum selection clause, which was included in the terms of use connected to Hotwire's ordering page via a hyperlink, to move litigation to Delaware. The plaintiff denied that he had ever agreed to the forum selection clause. Fortunately for the defendants, they were able to produce two declarations from employees at Hotwire affirmatively stating that the forum selection clause existed in the terms of use at the time the plaintiff booked his rental car and that the plaintiff could not have booked the rental without checking an "acceptance box" indicating his assent to the hyperlinked terms of use. Therefore, the court concluded, the plaintiff had notice of and consented to the terms of use containing the forum selection clause.

MODIFICATIONS

One of the most difficult issues relating to Website Terms involves modifications and updates. Website Terms typically include a provision granting the website owner the right to modify the terms unilaterally. This makes sense in practical terms; a website owner cannot be expected to continue to operate under the same terms indefinitely and it would not be feasible to negotiate every update with individual users. At the same time, however, Website Terms are contracts and, under black letter contract law, contract modifications require acceptance by both parties. A website operator ideally should require users to affirmatively accept each updated version of Website Terms, for example, by presenting the updated terms and requiring a click acceptance when the user first logs in after the change. But where obtaining such affirmative acceptance is not feasible, a website operator may nonetheless be able to enforce changed terms against users if it gives users sufficient notice of the change and informs them that continued use of the website constitutes acceptance.

For example, the plaintiff in *Rodriguez v. Instagram* (San Francisco Sup. Ct. Feb. 28, 2014), objected to certain changes in Instagram's terms of use. Instagram had unilaterally modified its terms in December 2012, and announced the changes to its users a month in advance of their implementation. The new terms stated that continued use of the website amounted to consent to the modifications, and that users who did not accept the modifications must stop using Instagram. The court found that, by continuing to use Instagram, Rodriguez agreed to the new terms, and that she could simply have stopped using Instagram if she did not want to be subject to them. The court pointed out that Rodriguez could not possibly have had a reasonable expectation of perpetual use of Instagram's service under the original terms, which included an express modification right for Instagram.

It should be noted, though, that courts in some cases have looked less favorably on website operators' attempts to modify Website Terms unilaterally, particularly where users are not given adequate notice or the changes are applied retroactively. For example, the Ninth Circuit held in *Douglas v. Talk America* (9th Cir. 2007), that an individual's assent to changed Website Terms could not be inferred where the individual had not actually received notice of the changes. In Douglas, the defendant Talk America provided long distance services to the plaintiff Douglas. When a dispute arose, Talk America attempted to enforce an arbitration provision contained in updated terms that it had posted to its website. But Talk America had never given Douglas notice of the updated terms and Douglas was not required to visit the Talk America website in order to continue using the Talk America services. The court noted, "[P]arties to a contract have no obligation to check the terms on a periodic basis to learn whether they have been changed by the other side."

Even more problematic for website operators, the court in *Harris v. Blockbuster, Inc.* (N.D. Tex. 2009), held that an arbitration clause in Blockbuster's online terms was illusory and unenforceable because Blockbuster reserved the right to unilaterally modify the terms and apply the modified terms to earlier disputes. Interestingly, Blockbuster had not actually modified its terms of use and attempted to apply the modified terms retroactively; rather, the court held that the mere reservation of the right to unilaterally amend the terms rendered the contract illusory. The court in *In re Zappos.com, Inc.* (D. Nev. 2012), came to a similar conclusion regarding the unilateral modification provision in Zappos' online terms of use (the Zappos court also did not look favorably upon Zappos' browsewrap implementation of its terms).

TAKEAWAYS

In light of the issues noted above, the following are some steps that website operators may take to increase the likelihood that Website Terms will be enforceable against site users:

- When possible, Website Terms should be implemented using clickwraps that give clear notice and require affirmative assent, rather than through browsewraps. If a browsewrap is used because a clickwrap is not feasible – e.g., where a website does not require users to register and does not otherwise include functionality to interact with users – website operators should present the terms as conspicuously as possible (and should recognize that their Website Terms may prove more difficult to enforce).
- If a clickwrap is used, website operators should be prepared to produce evidence that users must actually accept the Website Terms to access the website or make a purchase on the website, and be able to show the specific version of the Website Terms that were in place at the time that any given user indicated acceptance.
- A prominent notice should be included on the website regarding

the Website Terms and the terms should be easily accessible to users, including for download and printing. Website Terms should be easy for users to understand and particularly important terms—such as disclaimers, limitations of liability and dispute resolution provisions—should be conspicuous. Also consider adding a prominent "last updated" notice to Website Terms.

- When modifying Website Terms, consider obtaining users' express acceptance of the updated terms, if possible. If obtaining such express acceptance is not feasible, the users ideally should be provided with clear advance notice of any changes and a statement that continued use of the website following implementation of the updated terms constitutes acceptance of those terms.

- Regardless of how terms are updated, website operators should not assume that they will be able to enforce updated terms retroactively. Indeed, website operators should consider making clear in their Website Terms that newly added provisions will not apply to disputes arising prior to the adoption of the new provisions.

NEW CALIFORNIA PRIVACY LAW REVISIONS WILL IMPACT WEBSITE AND MOBILE APP OPERATORS WITH USERS UNDER AGE 18

By Julie O'Neill and Patrick Bernhardt

In 2013, California made child-related revisions to its Online Privacy Protection Act that have ramifications for websites and other online services that are not even directed to children. The revision, "Privacy Rights for California Minors in the Digital World," imposes obligations on any website, application, or other online service that (1) is directed to minors—that is, was created to reach an audience predominantly composed of minors—or (2) has actual knowledge that a minor is using it because, for example, it collects date of birth (each, a "Covered Service"). Cal. Bus. & Prof. Code §§ 22580-81. Covered Services are thus not limited to services directed to minors: even a general audience or adult-directed service is subject to the law if it collects age information and permits those who identify as minors to use the service. The law does not require an operator to collect age from its users.

The revised law will require a Covered Service to permit a registered user who is a minor to remove content that he or she has posted. It will also prohibit a Covered Service from advertising adult products to minors and from collecting, using, or disclosing minors' personal information for such advertising, or allowing others to do so.

The revised law takes effect on January 1, 2015. It will require a Covered Service to permit a registered user who is a minor to remove content that he or she has posted. It will also prohibit a Covered Service from advertising adult products to minors and from collecting, using, or disclosing minors' personal information for such advertising, or allowing others to do so.

THE DELETE BUTTON REQUIREMENT

The law will require a Covered Service to permit a registered user who is under 18 to remove content that he or she has posted to the service. Specifically, it will have to:

- Permit a minor to remove, or to request and obtain removal of, content that he or she has posted to the service ("posted" means that the content is accessible to others); and

- Provide instructions (e.g., in its privacy policy) on how a minor may remove or request removal of posted content, along with an explanation that removal does not ensure complete or comprehensive removal of the content.

Cal. Bus. & Prof. Code § 22581. The explanation that removal does not ensure complete or comprehensive removal is necessary because the law does not require removal in certain situations, including if another provision of law requires the Covered Service to maintain the content, if it was posted or reposted by users other than the minor, or if the minor received consideration in exchange for the posting. Cal. Bus. & Prof. Code § 22581(b)(1), (2), (5). Moreover, the law does not require permanent deletion of removed content. Rather, a Covered Service may comply with a removal request by: (1) anonymizing the content so that the minor cannot be individually identified; or (2) rendering the content invisible to others, while retaining it on its servers.

LIMITS ON ADVERTISING

The revised law also prohibits Covered Services from advertising adult products, such as alcohol, tobacco and firearms, to minors and from collecting, using or disclosing minors' personal information for such advertising, or allowing others to do so. Cal. Bus. & Prof. Code § 22580. This provision applies to a Covered Service that is directed to minors or that has actual knowledge

that the advertising will be targeted to a minor. If a Covered Service uses a service provider to deliver its advertising and notifies the service provider that the service is directed to minors, then the responsibility to comply with the law rests with the service provider. Cal. Bus. & Prof. Code § 22580(h)(1)-(2).

WHAT DOES THIS MEAN IN PRACTICE?

Each operator of a website, app or other online service should determine whether it falls within the law's coverage and, if so, develop a strategy to achieve compliance before the law takes effect on January 1, 2015. When doing so, we suggest:

- If you operate a general audience or adult-directed site or service and you do not have a business need for your users' age information, do not collect age or date of birth from your registered users on a going-forward basis. This will limit your need to comply, at least with respect to new users.
- If you operate a Covered Service and permit users to post information or content (such as through a profile, blog, chat, message board or similar feature), consider whether you will let registered users who are minors remove their posted content themselves or request to have it removed (or anonymized) by you. In either case, in your privacy policy, provide notice of the minor's right, along with instructions and an explanation that removal does not ensure complete removal. For example:

If you are under 18 and a registered Site user, you may ask us to remove content or information that you have posted to the Site by writing to [email address]. Please note that your request does not ensure complete or comprehensive removal of the content or information, as, for example, some of your content may have been reposted by another user.

- If you have actual knowledge that you are targeting advertising to minors, ensure that your advertising does not promote any of the adult products covered by the law.
- If you have actual knowledge that you have collected personal information from a minor, put policies and procedures in place to ensure that such information is not collected, used or disclosed—by you or any third party—to advertise adult products.
- If you operate a Covered Service that is directed to minors: (1) do not advertise adult products; (2) take steps to ensure that your users' personal information is not collected, used or disclosed—by you or any third party—to advertise adult products; and (3) inform your advertising service providers that your service is directed to minors.

COPYRIGHT: EUROPE EXPLORES ITS BOUNDARIES – NEW UK INFRINGEMENT EXCEPTIONS – THE ONES THAT CAME BACK AGAIN

By Chris Coulter and Mercedes Samavi

In June of this year, we sent out an alert about the anticipated new UK copyright infringement exceptions. These exceptions were to be introduced based on the recommendations of the Hargreaves Review. Surprisingly, some of the exceptions had been dramatically pulled from the legislative slate at the last minute. The UK government, however, has now upheld its subsequent promise to re-publish the statutory instruments for the infringement exceptions for (1) personal use, (2) parodies and (3) quotations, with new legislation on all three subjects that came into force on October 1, 2014.

Almost in parallel, a European ruling and an Advocate General opinion have helped to prepare for the arrival of the two statutory instruments, with commentary on (i) the scope of parody and (ii) in relation to personal use, the impact of copyright levies.

THE NEW LEGISLATION

Two new regulations have come into force, amending the Copyright, Designs and Patents Act 1988 (CDPA) to include new exceptions for copyright infringement. The first—the Copyright and Rights in Performances (Quotation and Parody) Regulations 2014 ("Quotation and Parody Regulations")—extends the provisions for quotations of copyright-protected works (having previously only been available for criticism and review), and creates a new provision for parodies. The second regulation—the Copyright and Rights in Performances (Personal Copies for Private Use) Regulations 2014 ("Personal Copies Regulations")—concerns making copies of copyrighted works for personal use.

QUOTATION

From October 1, 2014, the free quotation of copyright protected works is no longer limited to reporting current events or to works of criticism or review. The Quotation and Parody Regulations, inserted into the CDPA as section 30(1ZA), now permit quotation for any purpose, provided that:

- the work quoted has been made publicly available;
- the use of the quotations constitutes "fair dealing" with the work;
- the extent of a quotation is no more than is necessary for the purpose; and
- the quotation is accompanied by sufficient acknowledgment to the

copyright owner (unless this is impossible).

The UK Intellectual Property Office has stated that this amendment will help to save costs on copyright clearance, support free expression and align UK law with the rest of Europe. As anticipated in our previous alert, however, the Quotation and Parody Regulations do not provide a definition of "quotation," nor guidance as to how extensive a "quotation" is allowed to be. This may place undue pressure on the meaning of "fair dealing" as UK courts seek to define the scope of the exception.

PARODY

The new exception for parodies allows fair dealing with a work for the purposes of caricature, parody or pastiche (section 30A of the CDPA) and provides that fair dealing with a recording or performance (section 2A to Schedule 2 of the CDPA) for the purposes of parody does not infringe copyright conferred in the performance or recording. This change now means that the permission of the copyright holder will no longer have to be obtained, provided that the use of the original work is fair and proportionate. This is good news for British comedians and artists, it would seem, unless, of course, it is their work that is being parodied.

However, an EU court ruling on parodies in September 2014 has already placed some restrictions on the new legislation. In *Deckmyn v Vandersteen C-201/13*, the Court of Justice of the European Union (CJEU) defined a parody as something that evokes an existing work while being noticeably different from it and constituting an expression of humor or mockery. The CJEU also stated that national courts must strike a balance between copyright owners' interests and mimickers, and that copyright owners have a legitimate interest in disassociating their work from a parody, if the parody involves a discriminatory message.

This creates a whole new checklist for UK courts to consider, alongside the usual fair dealing test. Judges will have to also hold a view on whether the parody (i) strikes a fair balance, (ii) differs noticeably from the original work, and (iii) is sufficiently humorous. In particular, the last of these requirements may worry budding parodists, who could end up having to justify their comedy in front of a very different audience than first intended.

Two new regulations have come into force, amending the Copyright, Designs and Patents Act 1988 (CDPA) to include new exceptions for copyright infringement.

PERSONAL COPIES

The Personal Copies Regulations, incorporated into the CDPA as section 28B, now allow consumers to make personal copies of content (other than computer programs) they have bought, as long as (i) the copy is for their own private and non-commercial use, (ii) the copy is not an infringing copy, and (iii) the content has been lawfully acquired on a permanent basis. The UK government's hope is that this new exception will cause UK law to reflect common consumer practice more closely in this area.

The personal use exception contains some interesting features:

- Temporary vs. permanent copies – Any copies of works that have been borrowed, rented, broadcast, streamed or obtained using any other technology, which allows for only temporary access to a copy are not "lawfully" acquired and would not benefit from the exception. For example, copying a show from a TV streaming service is not allowed.
- Cloud services – Copies can be made for "back up" and "format-shifting," provided that the copy is accessible only to the individual and the data storage provider. This feature has been included, perhaps in an effort to assuage rights holders' concerns about P2P sites.
- Technological protection measures – To ensure that copyright owners do not unduly prevent copying of content for personal use, there is a procedure to submit complaints to the Secretary of State, in the event that a technological measure prevents a copyrighted work from being copied for personal use (see section 296ZEA of the CDPA).

It had been thought that there might be some concession made, such as copyright levies on storage media, to the "fair compensation" lobby that has complained that the personal use exception may cause financial detriment to rights holders. The UK government, however, has given no indication that any such compensation system is to be introduced. It is worth noting that some EU countries already have such levies in place; however, the decision whether to introduce levies lies with each Member State. This determination was reaffirmed in a recent Advocate General opinion in *Copydan Båndkopi v Nokia C-463/12*. A final decision in the case has not yet been issued, and we will consider the implications of the CJEU judgment on the UK position once a definitive ruling has been made.

CONCLUSION

The personal use exception remains controversial and faces criticism from rights holders such as musicians, who could lose out on approximately £58 million in revenues a year, as a result. Further, the relationship between the personal use exception and temporary content apps such as Snapchat poses interesting questions for users and companies alike.

There are no guidelines as to what constitutes a "quotation," and although there are guidelines as to what

constitutes "parody," the inherently subjective nature of aspects of those terms allows room for disagreement.

The initial uncertainties about the limits of the two new exceptions may trouble rights holders, especially adding the concern that users will be emboldened to stretch boundaries. This in turn seems likely to lead to judicial intervention. So, while the new exceptions align the UK more closely with other parts of Europe, commercially these changes may result in some copyright owners being forced into selective, strategic litigation in an effort to protect their works.

COUNTERFEIT GOODS: HAS THE WAR ON ISPS JUST GOTTEN TOUGHER?

By Sarah Wells and Chris Coulter

The pressure on ISPs to take responsibility for the sites accessible through their services has been growing in recent years (e.g., the requirement for certain ISPs to block filesharing sites). On October 17, 2014, the High Court of England and Wales took this one step further by granting a website-blocking order against certain ISPs in a case involving counterfeit goods. This case is notable for the fact that the infringement related to trademarks and not copyright. While English copyright law has a provision under which blocking injunctions may be sought, there is no statutory equivalent under trademark law, yet an injunction was still granted. Has the war on ISPs just gotten tougher?

The ISPs in question were Sky, BT, EE, TalkTalk and Virgin, and the matter centered around six websites that advertise and sell counterfeit goods (such as Cartier and Montblanc). The claimants (trademark owners in the Richemont/Cartier group) sought a blocking injunction from the ISPs for these six sites.

In reaching his decision to grant the blocking injunction, Mr. Justice Arnold focused on (a) whether the court had jurisdiction to grant the injunction; (b) whether such an injunction could be granted where no specific statutory legislation was in place relating to this remedy; and (c) whether the threshold conditions were met for granting such an injunction.

Having established that the court did indeed have jurisdiction, Mr. Justice Arnold noted that, although there is no specific legislation providing for injunctions in cases of trademark infringement, to grant such an injunction against a non-infringing party would nevertheless be consistent with EU law and UK policy. Further, Mr. Justice Arnold noted that "the 1994 [Trade Mark] Act both confers remedies against persons who are not necessarily infringers . . . and yet does not purport to contain a comprehensive code of the remedies available to a trade mark proprietor . . . More generally, there is nothing inconsistent between granting an injunction against intermediaries . . . and the provisions of the 1994 Act." Thus, in this instance, the court held that an injunction could be granted even where no specific statutory legislation was in place.

Mr. Justice Arnold noted that, although there is no specific legislation providing for injunctions in cases of trademark infringement, to grant such an injunction against a non-infringing party would nevertheless be consistent with EU law and UK policy.

Mr. Justice Arnold then focused on whether the threshold conditions for an injunction—in this case a website-blocking order—were met:

1. Is the defendant an intermediary within the meaning of Article 11 of the Enforcement Directive (Directive 2004/48/EC)? The court determined that ISPs clearly fall into this category.

2. Do the users and/or the operators of the website in question infringe the claimant's trademarks? The court determined that each of the six websites did infringe because each provided goods bearing signs identical to the trademarks in dispute, and sold these goods in response to orders without consent of the claimants.

3. Do users and/or the operators of the websites use the ISPs' services to infringe? Mr. Justice Arnold held that the answer to this question was yes. The ISPs have an essential role, as it is via their services that the advertisements and offers for sale are communicated to users in the UK. Even if UK consumers don't purchase any goods, the first act of infringement is already complete based just on the advertisements.

4. Do the ISPs have actual knowledge? Here again, the court held in the affirmative: If the operators of the websites in question use the ISPs' services to infringe, then the ISPs have actual knowledge of the infringement, based on the fact that the claimants sent notices to the ISPs and the other evidence produced.

In considering whether the injunction would unduly interfere with the ISPs' freedom to carry on business and Internet users' freedom to receive information, Mr. Justice Arnold considered that no new technology would be required to block the sites in question and, although alternative measures such as takedown and

deindexing were available, these measures would not be as effective as an injunction and would not be less burdensome. He did, however, adopt certain points made by the Open Rights Group, including requiring that additional information be provided to users when they attempt to access the blocked sites and limiting the order to an initial two-year period.

The Internet is increasingly used in the counterfeit goods trade. A study published in 2008 by the Organisation for Economic Co-operation and Development entitled *The Economic Impact of Counterfeiting and Piracy* estimated that the value of counterfeited and pirated goods moving through international trade alone in 2005 amounted to $200 billion. In 2014, the European Commission published its *Report on EU Customs Enforcement of Intellectual Property Rights: Results at the EU Border*, which recorded that, in 2012, customs authorities at the external borders of the EU seized a total of over 39.9 million articles, representing a market value of almost €900 million, with the UK seizing more articles than any other Member State. It remains to be seen, however, whether this case, acknowledged by Mr. Justice Arnold as a test case, will open the floodgates for trademark owners affected by this widespread issue or, given that domain names can be easily purchased and new sites quickly set up, will have little real impact.

If you wish to receive a free subscription to our Socially Aware newsletter, please send a request via email to sociallyaware@mofo.com. We also cover social media-related business and legal developments on our Socially Aware blog, located at www.sociallyawareblog.com.

For breaking news related to social media law, follow us on Twitter @MoFoSocMedia. To review earlier issues of Socially Aware, visit us at www.mofo.com/sociallyaware.