Volume 7, Issue 4, July 2016

SOCIALLY AWARE

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION

2011 BEST LAW FIRM NEWSLETTER

THE SOCIAL MEDIA LAW UPDATE

IN THIS ISSUE

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

John F. Delaney
Malcolm K. Dort
Adam J. Fleisher
J. Alexander Lawrence
Susan McLean
Christine E. Lyon
Julie O'Neill
Mary Race
Mercedes Samavi
Joshua R. Stein

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, we take a look at courts' efforts to evaluate emoticons and emojis entered into evidence; we describe the novel way one court addressed whether counsel may conduct Internet research on jurors; we examine a recent decision finding that an employee handbook provision requiring employees to maintain a positive work environment violates the National Labor Relations Act; we discuss an FTC settlement highlighting legal risks in using social media "influencers" to promote products and services; we explore the threat ad blockers pose to the online publishing industry; we review a decision holding that counsel may face discipline for accessing opposing parties' private social media accounts; we discuss a federal court opinion holding that the online posting of copyrighted material alone is insufficient to support personal jurisdiction under New York's long-arm statute; and we summarize regulatory guidance applicable to social media competitions in the UK.

All this—plus an infographic illustrating the growing popularity of emoticons and emojis.

MIXED MESSAGES: COURTS GRAPPLE WITH EMOTICONS AND EMOJI

By John F. Delaney

Emoticons—such as **:-)**—and emoji—such as 🤔🙄—are ubiquitous in online and mobile communications; according to one study, 74 percent of Americans use emoticons, emoji and similar images on a regular basis.

Given their popularity, it comes as no surprise that courts are increasingly being called upon to evaluate the meaning of emoticons and emoji that are included in material entered into evidence, an exercise that has highlighted just how subjective—and fact-specific—interpretations of these symbols can be.

> **If you want a message to be free from ambiguity, don't include an emoticon or emoji in the message.**

For example, in an opinion last year dismissing a male law school student's suit against local police and a female classmate for having the male student formally investigated based, at least in part, on text messages that he had sent, a federal district court in Michigan held that the male student's text messages showed that he may have had an intent to harass the female classmate despite "the inclusion of the emoticon, a '-D,' which appears to be a wide open-mouth smile." The court held that the emoticon "does not materially alter the meaning of the text message," in which the male student otherwise wrote that he wanted to do "just enough to make [the female student] feel crappy."

On the other hand, in a separate case, also arising in Michigan, the Michigan Court of Appeals held that the ":P" emoticon accompanying a comment allegedly accusing a city worker of corruption made it "patently clear that the commenter was making a joke."

Here are some other notable instances in which emoticons and emojis were among the evidence courts were asked to evaluate:

- In a sexual harassment case brought by the female co-CEO of a Delaware corporation against her partner, opinion issued last summer, the Delaware Chancery Court held that a "smiley-face emoticon at the end of [the defendant's] text message suggests he was amused by yet another opportunity to harass" the plaintiff.
- In the January trial of a California man accused of operating a black market called Silk Road over the Internet, the judge instructed the jury members that they should take into account the emoji included in the social media posts and other electronic communications submitted into evidence, stating that the emojis are "part of the evidence of the document." (The defendant, Ross Ulbricht, was ultimately convicted of all seven of the counts he faced; the government's evidence that he ran "Silk Road's billion-dollar marketplace under the pseudonym the Dread Pirate Roberts was practically overwhelming.")
- In a petition for *certiorari* by Anthony Elonis, a Pennsylvania man whose conviction for posting threatening status updates to Facebook was ultimately overturned by the U.S. Supreme Court last year, Elonis cited his inclusion of the emoticon ":-P" several times as part of his arguments that:
  (1) he lacked the intent required for conviction; and (2) his posts were easily misunderstood, and communications that are subject to misunderstandings shouldn't be criminalized. Holding that "Elonis's conviction was premised solely on how his posts would be viewed by a reasonable person, a standard feature of civil liability in tort law inconsistent with the conventional criminal conduct requirement of "awareness of some wrongdoing."" The Supreme Court's opinion didn't mention emoticons at all, however.

Each of these decisions involved a court's assessment of a lengthy set of facts, of course. Context clearly counts. The point is that, in the words of *WIRED's* Julia Greenberg, "When the digital symbol for a gun, a smile, or a face with stuck-out tongue comes up in court, they aren't being derided or ignored. Emoji matter."

Interpreting them will continue to be a challenge for courts. Emoticons and emojis are often ambiguous, sometimes supporting the accompanying text, sometimes undermining it. A smiley face with a tongue sticking out that accompanies a message purporting to confirm a deal could indicate the sender's happiness that the deal has been concluded, or it could indicate that the sender's purported confirmation is a joke.

Further complicating the interpretation of emojis is the fact that the same emoji character will have a different appearance when viewed on different platforms. For example, the popular "grinning face with smiley eyes" emoji that, say, a Microsoft platform user sees is not identical to the "grinning face with smiley eyes" emoji that, say, a Google platform user sees—even if the emoji was sent by the former to the latter. Moreover, a recent study found that the differences in an emoji's appearance across platforms can result in different emotional responses to the emoji based on the platform from which it is viewed. As a result, a court seeking to interpret an emoji

92%

of the people who use the Internet use emoji.[1]

More than 30% of the people who use emoji use them several times a day.[1]

12% — 40% of the top brand pages on Facebook included emoji in their posts in Q4 of 2015, up from 28% in Q4 2014.[2]

14% — 59% of the top 500 brands on Twitter sent out tweets that included emoji in Q4 of 2015, up from 45% in Q4 2014.[2]

45% 14% 13% 5%

45% of the emoji texted by Android and iOS users are happy faces, making that emoji the most popular, followed by sad faces (14%), hearts (13%) and hand gestures (5%).[3]

Australia's use of emoji that fall into the alcohol category is twice the worldwide average (.80% vs. .41%).[4]

SOURCES

1. http://www.adweek.com/news/advertising-branding/infographic-emojis-are-becoming-preferred-communication-tool-across-demographics-167355
2. http://www.socialbakers.com/blog/2510-emoji-marketing-is-growing-fast
3. http://www.huffingtonpost.com/2015/04/22/emoji-report-will-bear-your-soul-to-the-world_n_7116706.html
4. https://www.scribd.com/doc/262594751/SwiftKey-Emoji-Report

will need to determine in each situation which version of the emoji to consider: the version that appeared to the sender of the communication at issue or the version that appeared to the recipient of that communication?

It's been said that one shouldn't send a message that he or she wouldn't want to see on the front page of the *New York Times*. I'd like to suggest a corollary rule: If you want a message to be free from ambiguity, don't include an emoticon or emoji in the message.

JUDGE IN HIGH-PROFILE CASE OBTAINS ATTORNEY AGREEMENT NOT TO ENGAGE IN JUROR SOCIAL MEDIA SNOOPING

By Malcolm K. Dort and J. Alexander Lawrence

It seems that almost everyone uses social media nowadays. Of course, this means that most every juror is a social media user, as well as that courts are dealing with the thorny questions that arise out of the proliferation of social media usage among jurors.

Like the long-standing practice of warning jurors not to talk about the case with friends and family or to read press reports about the case during the course of trial, courts now routinely caution jurors not to send messages about the case through social media, tweet about the case or look for reports about the case on social media sites. Courts are also taking notice of the potential pitfalls that arise when attorneys poke around prospective jurors' social media sites to try to decide who may be a friendly (or unfriendly) juror.

Recently, a federal court in the Northern District of California addressed this subject in the high-profile copyright case *Oracle v. Google*. The case concerns allegations that Google unlawfully incorporated parts of Oracle's copyrighted Java code into the Android operating system.

In a recent order, the court asked counsel for Oracle and Google to refrain from conducting any Internet research on potential or empaneled jury members prior to the trial verdict. Because an outright ban would have the unintended consequence of prohibiting the lawyers for the parties—but no one else in the courtroom—from accessing online information on the jurors, the court opted instead to seek the parties' agreement to a voluntary ban. As added incentive to reach agreement, the court offered counsel for both sides extra time to screen potential jurors during voir dire. Both parties ultimately agreed to the voluntary ban.

The court cited three reasons to support its decision to seek the ban.

[C]ourts now routinely caution jurors not to send messages about the case through social media.

First, the court reasoned that jurors, upon learning that counsel was investigating them, might be tempted to investigate the lawyers and the case online themselves. Further because there is plenty of information online about the high-profile dispute, the court saw an "unusually strong need" to deter any jury member from conducting out-of-court research. The court noted, for example, that a Google search for "Oracle v. Google" yields almost one million hits, and that both parties have hired online commentators to promote their respective sides of the case on blogs and other websites. Because the large amount of online commentary in particular could present a significant risk to a fair hearing, a ban would help ensure that the jury reaches a verdict on the basis of trial evidence only.

Second, the court ruled that online jury research could enable counsel to make "improper personal appeals" to individual jurors during jury argument. For instance, if counsel learns through a social media search that a juror's favorite book is To Kill a Mockingbird, counsel could, in an attempt to capture the attention of an empaneled juror, craft an argument regarding copyright law that weaves in references to that book and the recent death of Harper Lee. The court reasoned further that such calculated appeals would be "out of bounds" because the judge might not "see what was really in play."

Third, a voluntary ban would protect the privacy of potential jurors. Because "[t]hey are not celebrities or public figures," the court ruled that the privacy of potential jurors should not be invaded except to reveal bias or a disinclination to follow court instructions. In anticipation of the argument that potential jurors choose to expose themselves to public scrutiny through their social media privacy settings, the court ruled that "understanding default settings is more a matter of blind faith than conscious choice."

The court's approach creates new precedent in the area of jury selection procedure, where, to date, parties have been left with little guidance. Indeed, the court itself recognized that "there are precious few decisions" that address the specific issue of whether counsel may conduct Internet and social media research on jurors in their cases.

Existing guidance on this issue stems largely from the American Bar Association (ABA), which has stated that counsel's "passive review" of a juror's website or social media profile, while refraining from making access requests to jurors, does not violate ethical rules on *ex parte* jury communications. That being said, even the ABA has cautioned that courts may limit social media research in certain cases.

Similarly, the New York State Bar Association (NYSBA) advised recently that, prior to jury selection, judges should address and resolve, on a case-by-case basis, use of social media by attorneys for the purpose of investigating jurors. Relevant questions to consider include what social media services attorneys may review; which social media platforms counsel or his/her reviewing agent (e.g., a jury consultant) is a member of; and whether results of social media monitoring will be shared with opposing counsel and the court.

The Oracle v. Google decision represents a key step toward marking clear boundaries for social media and Internet investigation by counsel. Further, the decision shows that, left unchecked, online jury research could lead to improper jury appeals, unwarranted privacy invasions and—perhaps most importantly—compromise of the fair trial process.

As social media use continues to proliferate, we can expect that courts and bar associations will provide further guidance on how attorneys can properly use social media to research the background of both prospective and sitting jurors.

DON'T WORRY, BE (UN)HAPPY: DOES U.S. LABOR LAW PROTECT A WORKER'S RIGHT TO A BAD ATTITUDE?

By Christine E. Lyon and Mary Race

A few months ago, we noted that a Yelp employee's online "negative review" of her employer might be protected activity under the National Labor Relations Act (NLRA), given that the National Labor Relations Board (NLRB) has become increasingly aggressive in protecting an employee's right to discuss working conditions in a public forum, even when that discussion involves obscenities or disparaging the employer. This trend has prompted us to report previously on the death of courtesy and civility under the NLRA.

Now, the NLRB has confirmed that it is not only courtesy and civility that have passed away—a "positive work environment" has perished with them.

A recent NLRB decision found that T-Mobile's employee handbook violated the NLRA by requiring employees "to maintain a positive work environment by communicating in a manner that is conducive to effective working relationships with internal and external customers, clients, co-workers, and management."

According to the NLRB, employees could reasonably construe such a rule "to restrict potentially controversial or contentious communications," including communications about labor disputes and working conditions that are protected under the NLRA. The NLRB concluded that employees rightly feared their employer would consider such communications to be inconsistent with a "positive work environment." Similarly, the NLRB struck down T-Mobile's rules against employees "arguing" and making "detrimental" comments about the company.

> Encouraging a positive attitude among employees could have negative results.

The main sticking point appears to be requiring employees to be "positive" towards co-workers and management. Earlier NLRB cases have indicated that requiring employees to be courteous only towards customers may not set off as many NLRB alarm bells. Nonetheless, employers should tread carefully—and try not to be too cheerful. Encouraging a positive attitude among employees could have negative results.

INNOVATIVE SOCIAL MEDIA MARKETING CANNOT OVERLOOK OLD-FASHIONED COMPLIANCE

By Julie O'Neill and Adam J. Fleisher

Social media is all about innovation, so it is no surprise that social media marketers are always looking for innovative ways—such as courting social media "influencers" and using native advertising—to promote products and services to customers and potential customers. However, as the retailer Lord & Taylor recently learned, the legal rules that govern traditional marketing also apply to social media marketing.

Earlier this year, the Federal Trade Commission (FTC) reached a settlement with Lord & Taylor in a dispute involving its online advertising practices (the final consent order was just approved by the FTC in late May 2016). According to the FTC's Complaint, Lord & Taylor allegedly:

- gifted a dress to 50 "fashion influencers" and paid them to post on their Instagram accounts photos of themselves in the dress during a specified time frame; and
- paid for, reviewed and preapproved Instagram posts and an article in an online magazine, *Nylon*.

In neither case, according to the FTC, was Lord & Taylor's role in the promotional effort appropriately disclosed.

On these alleged facts, the FTC brought three counts alleging the following violations of Section 5 of the FTC Act's prohibition on deceptive practices:

- the failure to disclose that the influencers' Instagram posts did not reflect their independent and impartial statements but rather were specifically created as part of an advertising campaign;
- the failure to disclose or adequately disclose that the influencers were paid endorsers; and
- the failure to disclose that the *Nylon* materials were not independent statements and opinions of the magazine but rather "paid commercial advertising."

As has been widely remarked, this is not the first time the FTC has brought a case relating to social media advertising. The settlement, however, is noteworthy because it brings together issues relating to both native advertisements and endorsements. The FTC has been focusing on these issues since late 2014; its activities have included:

- Settling with the advertising firm Deutsch LA, Inc. in late 2014 in connection with its allegedly deceptive activities relating to the promotion, on behalf of its client, Sony, of the PlayStation Vita handheld gaming console through Twitter (we wrote about the Deutsch LA case on Socially Aware).
- Settling in September 2015 with Machinima, Inc., an online entertainment network that allegedly paid video bloggers to promote the Microsoft Xbox One system (we also wrote about the Xbox One settlement on Socially Aware).
- Issuing a closing letter, at the same time as the Machinima settlement, indicating that the FTC had investigated Microsoft and Microsoft's advertising agency, Starcom, in relation to the influencer videos at issue in Machinima. The closing letter was significant because it suggested that the FTC was primed to take the position that a company whose products are promoted bears responsibility for the actions of its ad agencies—as well as the actions of those engaged by its ad agencies.
- Releasing a policy statement and guidance on native advertising in late 2015, which warned companies—again—that it is deceptive, in violation of Section 5, if reasonable consumers are misled as to the true nature or source of an advertisement. (Our Client Alert on these materials can be read here.)

The compliance issue with native advertising is that content that does not appear to be advertising—such as an advertisement or promotional article in an online or print publication formatted to look like the non-advertising materials in the same publication—must be clearly and conspicuously disclosed as advertising. The relevant compliance issue with endorsements is that any payment or other compensation received by the endorser from the promoter must be appropriately disclosed.

The concept underlying native advertisements and endorsements is the same: Consumers must be aware that they are reviewing promotional material, not "native" or "organic" content, whether it is on a social media platform, a website or in a print publication.

The Lord & Taylor settlement is yet another clear signal that paid promotions of any kind, in any medium, must be disclosed. Given the FTC's focus on these issues and the repeated enforcement actions, especially with respect to social media endorsements, it is likely that the FTC will continue to enforce in this area until it is convinced that the market understands the disclosure rules.

In light of the risk in this area, the Lord & Taylor Consent Order is noteworthy, as it provides valuable insight into how the FTC expects companies to avoid running afoul of the endorsement and native advertising rules.

For example, the Order requires Lord & Taylor to provide any endorser "with a clear statement of his or her responsibility to disclose, clearly and conspicuously," the material connection between the retailer and the endorser in any advertisement and communication and to obtain a signed and dated acknowledgment of receipt of this statement from the endorser. In addition, the Order requires Lord & Taylor to maintain a system to monitor and review its endorsers' representations and disclosures. Taken together, these requirements essentially lay out components of a compliance program that any company using social media for advertising should consider.

Of course, any such program requires time and resources, and no company has those in infinite supply. However, moving beyond the FTC's Complaint and Order, there are other noteworthy aspects of the social media endorsement issue that appear to have been overlooked.

Given the FTC's focus on these issues and the repeated enforcement actions, especially with respect to social media endorsements, it is likely that the FTC will continue to enforce in this area until it is convinced that the market understands the disclosure rules.

According to news reports and comments from Lord & Taylor, it appears that the company (and commentators) recognized the potential FTC compliance issue right after the ad campaign launched. The company reportedly stated, after the settlement, that "it came to our attention [a year ago] that there were potential issues with how the influencers posted about a dress in this campaign, [and] we took immediate action with the social media agencies that were supporting us on it to ensure that clear disclosures were made." Indeed, articles from the time of the advertising campaign noted, for example, that "the [endorsing] bloggers left out an important piece of information in their Instagram posts: a disclosure that they had been paid to post by Lord & Taylor." Another website commented at the time that the bloggers "failed to mention they were paid" and suggested that the company was getting away with violating the FTC Act (though it did note that many bloggers had gone back to add "#sponsored or #ad to their posts.)" The immediate aftermath of the Lord & Taylor campaign that ultimately formed the FTC's case suggests that awareness of the issues is rising among the public and that even a quick fix can be too late.

In light of this awareness, the failure to disclose obvious ties between the endorser and the promoter can undermine a campaign. Further, even though the FTC does not have the authority to impose civil money penalties for these types of violations of the FTC Act, state Attorneys General appear to be getting in on the act. Machinima, Inc., for example, settled allegations with the FTC regarding its use of influencers in promoting the Xbox One (as we noted above). A few months later, however, the company entered into a settlement with the New York Attorney General that included a penalty of $50,000 for its alleged failure to disclose payments to the influencers.

These events strongly suggest that ensuring appropriate disclosures is more than just an FTC compliance issue. While the FTC is actively enforcing in this space, the margin of error is shrinking not only because of the FTC, but also because of the increasing awareness of the public and the new risk of enforcement (including financial penalties) by state Attorneys General.

WILL AD BLOCKERS KILL ONLINE PUBLISHING?

By John F. Delaney

The Internet contains over 4.6 billion web pages, most of which are accessible for free, making content that we used to have to pay for—news, videos, games—available without having to hand over a credit card number.

What makes all of this possible is online advertising. As Internet industry commentator Larry Downes has noted, “If no one views ads, after all, advertisers will stop paying for them, and without ads the largely free content of the Internet has no visible means of financial support.”

The deal is pretty simple: We put up with the ads, and, in return, we get free access to a bottomless pool of content.

This system worked well for two decades. And then along came ad blockers—software that allows Internet users to avoid online advertisements by targeting the technology used to deliver the ads, the URLs that are the source of the ads or the mechanisms that enable the ads (even video ads) to be displayed in a certain way.

A GROWING THREAT TO ONLINE PUBLISHERS AND ADVERTISERS

The use of ad-blocking technologies by consumers grew by 41 percent over the past 12 months; there are now nearly 200 million active users of such technologies worldwide. In the United States, an estimated 45 million Americans are surfing an ad-free version of the Internet.

The use of ad blockers cost publishers an estimated $22 billion in 2015. That's because each Internet user is worth an estimated $215 a year in revenue from online ads, and—as heavy Internet users—people who use ad blockers are likely worth even more.

Moreover, the situation is growing worse as more people embrace ad-blocking technologies; the damage inflicted this year is expected to be over $41 billion.

Nor do consumers seem concerned by the threat that ad blockers pose to the Internet ecosystem; according to one survey, a mere two percent of Web surfers expressed a willingness to pay for ad-free access to online content.

WHAT'S A BELEAGUERED PUBLISHING INDUSTRY TO DO?

As more consumers adopt ad blockers, publishers are searching for ways to curtail the harm to their businesses. Unfortunately for publishers, many of the solutions being considered are unlikely to alleviate the problem.

Litigation against ad-blocker vendors is one option, but the chance of success may be low. No major lawsuits against ad blockers have been filed in the United States, but in Germany, where at least six publishers have sued Eyeo, the owner of Adblock Plus, the courts have held each time that ad blockers are legal.

> **The use of ad-blocking technologies by consumers grew by 41 percent over the past 12 months.**

Some publishers are looking for technological solutions to the problem. *The New York Times*, for example, is reportedly exploring the use of technical mechanisms to thwart ad-blocking software, but so far there's been no word on the success of those technical mechanisms. One imagines, however, that any blocker-busting technology adopted by the publishing industry will simply spur the creation of next-generation ad blockers designed to circumvent such technology.

“Native advertising” was once viewed as a promising strategy for sneaking ads past ad-blocking technology. Characterized as advertising that “follows the natural form and function of the user experience in which it is placed,” native advertising is often called “sponsored content” or an “advertorial.” But ad blockers have become more effective at suppressing native ads, with help from Federal Trade Commission rules that limit online advertising from too closely resembling editorial content.

Out of frustration, some content providers have turned to brute force to combat ad blockers. *Forbes*, for example, is walling off all ad-blocking Internet users from its Forbes.com site. Others have taken a softer approach, appealing to their site visitors to resist blockers.

MORE PROMISING APPROACHES?

A better solution than the approaches discussed above is for online advertising to become more compelling and less obtrusive. Improving consumers' online advertising experiences might be the publishing industry's answer to the ad-blocker problem because, while a majority of the consumers who install ad blockers do it because they find most ads distracting and useless, a sizable portion of ad-blocker users have expressed an appetite for some online ads.

While 45 percent of the ad-blocker users surveyed in one recent survey said they installed the software because they find the ads annoying (as opposed to installing it to stop online ads from compromising their privacy or the speed of their Internet connections), 30 percent said they block ads in order to remove only “a subset of specific advertising.” PaigeFair, the self-described “ad-blocking solutions” company that conducted the study that produced all of these statistics, advises marketers to “tailor an appropriate advertising experience” to that 30 percent.

Syracuse University advertising professor Brian Sheehan writes that one way to improve consumers' experiences with online advertising is to “vastly improve native advertising,” not because it will prevent ad blockers from working, but because, when it's done with sufficient “flair, relevance and journalistic integrity,” native advertising can become “terrific content” and “a great read.” In other words, it could become

> [T]he situation is growing worse as more people embrace ad-blocking technologies; the damage inflicted this year is expected to be over $41 billion.

advertising that consumers value and don't necessarily want to block.

Yet one has to wonder if marketers have the discipline to commit to creating more subtle, less obtrusive ads. If anything, the trend has certainly been in the opposite direction toward in-your-face ads that are impossible to overlook. Even if advertisers were suddenly to tone down their act, it's questionable whether the explosive growth of ad blockers can be reversed. Will Internet users, having grown accustomed to having their cake and eating it, too, be willing to abandon or even curtail their use of ad blockers? It seems unlikely.

Many advertisers and publishers are seeking to make online ads more palatable by creating bespoke online advertising experiences.

The Guardian, for example, is reportedly working with the Interactive Advertising Bureau to implement a customized ad experience that "puts the user in control." James Harris, chief digital officer of the European media giant Carat, applauds the move, noting that "the rise of ad blocking is partly due to the industry 'hitting people with bad-quality ads numerous times, via programmatic trading.'"

But it's hard to believe that bespoke advertising will stop web users from employing ad blockers. The more ads are tailored to individual users' interests, the greater the potential "creepiness factor" for many such users, driving them to install ad blockers. It's a catch-22 for the interactive industry: Users hate generic, irrelevant ads, but they dislike highly targeted, directly relevant ads as well.

THE END OF THE WEB AS WE KNOW IT?

With no real solution for reversing or even slowing the ad-blocking trend, the free web model is headed toward major disruption. Currently, 16 percent of U.S. web surfers use ad blockers—what happens when that number surpasses 30 percent, as it has in parts of Europe, or reaches 50 percent?

One thing is certain—for publishers, ad blockers are becoming the ultimate killer app. Without advertiser support, the amount of professionally produced, high-quality content made available online will decrease over time. By definition, professional content costs money to create and, without a return on investment, such content will disappear behind pay walls or just disappear.

We've seen how the rise of online publishing has led to the near demise of traditional publishing. But who could have anticipated that the online publishing industry would so quickly find itself facing its own existential threat?

This article is an expanded, "director's cut" version of an op-ed piece that originally appeared in *MarketWatch*.

NEW JERSEY SUPREME COURT QUESTIONS ETHICS OF "FRIENDING" A LITIGATION FOE

By Malcolm K. Dort and J. Alexander Lawrence

Attorneys often research adverse parties online to obtain potentially useful—and publicly available—evidence for use in a case. However, as an ethical matter, may an attorney access information available only through an adversary's private social media account?

The New Jersey Supreme Court just considered this question in a professional-misconduct complaint involving "Facebook spying" of a plaintiff by opposing counsel. In a recent ruling, the court held that attorneys who access an opposing party's private Facebook account without proper consent may face discipline for unethical conduct.

The disciplinary case arises out of a personal injury matter, in which the plaintiff sued the borough of Oakland, New Jersey, over injuries he sustained after allegedly being hit by a local police cruiser in 2007. Although the plaintiff had a private Facebook page, the borough's defense attorneys enlisted a paralegal at their firm to send a Facebook friend request to the plaintiff. The paralegal did not identify herself as an agent of defense counsel, and the plaintiff accepted the paralegal's request without realizing that she worked for the borough's counsel.

But when the defense attorneys later sought to introduce printouts of the plaintiff's Facebook page at trial and included the paralegal on their witness list, the plaintiff realized that defense counsel had been spying on him through the paralegal.

The plaintiff brought the conduct of defense counsel to the attention of the New Jersey Office of Attorney Ethics, which is now investigating the matter. The Office of Attorney Ethics alleges in a complaint filed with a state ethics committee that defense counsel had violated numerous New Jersey Rules of Professional Conduct. These violations include, for example, improper communication with a person represented by counsel, failure to supervise a non-lawyer assistant and engaging in "dishonesty, fraud, deceit, or misrepresentation." The defense attorneys claim that they acted in good faith and that they were unfamiliar with the privacy settings on Facebook.

To be clear, no final decision has been issued on the merits of this case, as the New Jersey Supreme Court's ruling confirms only that the Office of Attorney Ethics has discretion to review the ethics complaint. The case will now proceed to a merits hearing.

Engaging in subterfuge to gain access to the private social media site of an adversary is likely to get you into hot water.

But even if New Jersey has yet to rule definitively on the ethics of social media spying, existing guidance offers a cautionary note. For example, the New York City Bar Association has stated that "[a] lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent." Similarly, the Massachusetts Bar Association has stated that party counsel may "friend" an unrepresented adversary only when that lawyer discloses his or her identity as the party's lawyer. Likewise, the Philadelphia Bar Association has held that an attorney may seek access to the private social media page of a witness only by doing so "forthrightly" or by revealing that he or she is an attorney in the litigation.

Attorneys would do well, therefore, to ensure that they do not contact an adversary on social media—and especially not without first identifying whom they represent. Engaging in subterfuge to gain access to the private social media site of an adversary is likely to get you into hot water.

DO NOT GO GENTLE INTO THAT JURISDICTION: NO "SITUS OF INJURY" MERELY BECAUSE COPYRIGHTED MATERIAL IS ACCESSIBLE

By Joshua Stein and J. Alexander Lawrence

Because content posted online can be accessed nearly anywhere, courts regularly face the issue of whether they have personal jurisdiction over a defendant who posted material to the web or a social media site. Recently, one New York federal court held that the mere fact, standing alone, that copyrighted material posted online was accessible in New York did not create a "situs of injury" sufficient to support personal jurisdiction under New York's long-arm statute.

In *Pablo Star Ltd., et al. v. The Welsh Government, et al.*, the Ireland and UK-based owners of the copyright of two photographs of poet Dylan Thomas sued the Welsh government and its "Visit Wales" tourism bureau, as well as a number of content publishers, including the Tribute Content Agency, LLC, the Pittsburgh Post-Gazette and the Miami Herald Media Co. While the Welsh government defendants were dismissed on sovereign immunity grounds, the court was left to consider whether it had personal jurisdiction over the publisher defendants, none of which were based in New York.

The court quickly rejected any arguments regarding general personal jurisdiction, which renders a defendant amenable to suit on all claims that could be asserted in a jurisdiction. The court recognized that establishing general jurisdiction is exceedingly difficult under prevailing Supreme Court precedent.

Thus, the court turned to New York's long-arm statute, which, among other bases for obtaining jurisdiction over a defendant, would require "a tortious act [outside] the state causing injury to person or property within the state."

The court found that, because intellectual property is intangible, the injury in copyright or trademark infringement is generally in the state where the intellectual property is held—that is, the domicile of the owner of the intellectual property at issue. The court held that because the plaintiffs are foreign corporations, the situs of the injury cannot be New York.

Plaintiffs argued that they were injured in New York "specifically due to lost or threatened business" as they were "deprived [of] the potential opportunity to license and publish their copyrighted photos here." The court rejected this argument on two grounds.

The *Pablo Star* case teaches that copyright owners cannot simply point to the fact that material has been posted online and sue anywhere in the United States.

First, as a matter of principle, such a "market harm" theory could justify jurisdiction "anywhere that the internet is accessible," opening up a defendant to being sued anywhere and everywhere. Moreover, unlike most tort cases, where the location of plaintiff's injury is often singular and identifiable, the injury in online copyright infringement cases is "difficult, if not impossible" to pinpoint to a particular geographic region.

Second, the court reasoned that, to the extent identifiable, the injuries in this case are the fees that should have been paid by the publisher defendants—none of which are based in New York. Therefore, the simple fact that "New Yorkers can access the infringing content online" is insufficient to establish personal jurisdiction in New York.

The *Pablo Star* case teaches that copyright owners cannot simply point to the fact that material has been posted online and sue anywhere in the United States. Copyright owners must still establish personal jurisdiction over each defendant they sue for infringement. In cases like this—in which a foreign copyright owner named defendants as seven separate publishers that are located in various jurisdictions—a copyright owner may need to bring separate actions in different jurisdictions against each defendant. While onerous for foreign copyright owners, the outcome protects against hauling a defendant into a jurisdiction under which it may have few connections.

SOCIAL MEDIA COMPETITIONS IN THE UK: PLAY FAIR

By Susan McLean and Mercedes Samavi

With 1.65 billion users on Facebook, 332 million users on Twitter and 400 million on Instagram, it is unsurprising that many companies are seeking to increase brand awareness and customer engagement by running competitions via social media. If you want to avoid attracting the scrutiny of UK regulatory authorities, however, you will want to ensure that your social media competition complies with the Committee of Advertising Practice Code ("CAP Code").

The CAP Code acts as the rulebook for non-broadcast advertisements in the UK and requires that promotions (including those on social media) be legal, decent, honest and truthful. The Cap Code is enforced by the Advertising Standards Authority, the independent regulator responsible for advertising content in the UK. Given the particular challenges posed by social media, CAP has some useful guidance on sales promotions: prize draws in social media ("Guidance").

If you are running a prize promotion in the UK, it's important to become familiar with the CAP Code and Guidance to ensure that your competition doesn't run into legal problems. Here's a quick overview of some of the key principles set out in the Guidance.

> In addition to awarding any advertised prizes, adequate steps must be taken to ensure that the winner is notified. Calling a winner once, or only announcing the winner once via social media, is not sufficient.

KEY PRINCIPLES UNDER THE GUIDANCE

If you're organizing a promotion on social media, be sure that:

- the promotion is run equitably, promptly and efficiently;
- you deal fairly and honorably with participants;
- you avoid causing unnecessary disappointment; and
- any marketing communications connected with the promotion are not misleading.

In addition, the Guidance advises promoters to comply with the following practices:

1. **Include significant information in the initial advert.**

   Significant information includes the closing date, instructions on how to enter and any other restrictions on entry. Depending on the circumstances, other key information could include the start date, the number and nature of the gifts and/or prizes and the promoter's name and address.

   There is an exemption for platforms that severely restrict the space of the initial ad, such as Twitter, which limits posts to 140 characters. However, you are expected to include as much information as is practicable.

2. **Include a link to the full T&Cs.**

   All participants must be able to access the full terms and conditions ("T&Cs") that apply to the promotion before entry. These T&Cs must provide certain information, which participants must be able to access easily during the promotion period.

3. **Include all eligible entrants when selecting winners.**

   You must be able to demonstrate that a reliable method was used to collect all eligible entries (particularly where the method of entering requires using some feature of the applicable social media platform, such as re-tweeting a post on Twitter).

4. **Select prize draw winners at random.**

   This must be done in a verifiably unbiased way, for example, through the use of a computer process or in the presence of an independent person.

5. ***(You would think that it goes without saying but...)* Actually award the prize.**

   In addition to awarding any advertised prizes, adequate steps must be taken to ensure that the winner is notified. Calling a winner once, or only announcing the winner once via social media, is not sufficient.

If you are running a prize promotion, you will need to keep in mind legal issues that may affect the competition in addition to the ones addressed by the CAP Code, such as:

- Gambling – Ensure that the promotion does not constitute an unlawful lottery under the Gambling Act 2005. Prize draws that are free to enter (or offer at least one free method of entry) generally avoid being so classified under the Act.
- Data Protection – Your collection and use of participants' personal data must comply with data protection law. Ensure that your data processing is compliant and include a link to the applicable privacy policy in your T&Cs for the promotion.

PLATFORM-SPECIFIC RULES

The social media platform that you are using to run your prize promotion likely has its own rules regarding prize promotions. Make sure that you check the platform's rules before you run your promotion (the rules are regularly updated). If you breach the platform's rules, then you risk having your account disabled.

Here are some of the rules governing prize promotions that you will find in Facebook's, Twitter's and Instagram's terms of use.

Facebook

- Promotions must include an acknowledgement that the promotion is not affiliated with or endorsed by Facebook.
- Personal timelines or friend connections cannot be used to administer promotions. For example, you can't require participants to share posts on their timelines, or their friends' timelines, or tag their friends in posts in order to participate in the promotion.
- Pages promoting the private sale of certain goods, such as alcohol, tobacco and adult products, must restrict access to those aged 18 and older.
- Promotion of online gambling, casinos, lotteries and other related activities require prior authorization from Facebook and are only permitted in certain countries.

Twitter

- Discourage the creation of multiple Twitter accounts, for example, by including a rule stating that participants using multiple accounts will be ineligible to enter.
- The Twitter rules prohibit the posting of duplicate, or near duplicate, Tweets, links or updates, so don't encourage participants to duplicate tweets. Play it safe by having your competition's rules state that multiple entries submitted in a single day will not be accepted.
- To help ensure that all entries are counted, ask participants to include an @reply in their updates. This will help ensure that all tweeted entries show up in public searches.

Instagram

- Don't inaccurately tag, or encourage users to inaccurately tag, any content. This includes requesting users tag themselves in photos when they are not in the photo.
- Promotions must include an acknowledgement that the promotion is not affiliated with or endorsed by Instagram.

Conclusion

Running a social media competition can be an effective way to generate attention for your brand. By following the rules, you can help ensure that your brand is trending on Twitter, Facebook or other social media platform for all of the right reasons.

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.
