Volume 5, Issue 5, August 2014

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION
2011 BEST LAW FIRM NEWSLETTER

IN THIS ISSUE

EDITORS

John F. Delaney
Gabriel E. Meister
Aaron P. Rubin

CONTRIBUTORS

Ann Bevitt
Erin M. Bosman
Enrico Granata
Tiffany Hu
Lincoln Lo
Whitney McCollum
David McDowell
Susan McLean
Aaron P. Rubin
Joanna L. Simon
Jenny Wang
Craig Whitney

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

In this issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media, we examine the use of the Computer Fraud and Abuse Act to combat web scraping; we explore the launch of Google Glass in the UK and the issues it raises; we analyze the FDA's latest attempt to provide direction for drug and device manufacturers concerning how and when they may use social media; we report on a recent case concerning whether service providers can avail themselves of certain DMCA safe harbors; we highlight the increasingly important role of social media services in proxy contests; we take a look at how the Supreme Court's *Aereo* decision might impact other areas of technology; and we discuss the ongoing controversy regarding website accessibility under the ADA and California's Unruh Act.

All this—plus a collection of thought-provoking statistics about social media and the World Cup . . .

DATA FOR THE TAKING: USING THE COMPUTER FRAUD AND ABUSE ACT TO COMBAT WEB SCRAPING

By Tiffany Hu and Aaron Rubin

"Web scraping" or "web harvesting"—the practice of extracting large amounts of data from publicly available websites using automated "bots" or "spiders"—accounted for 18% of site visitors and 23% of all Internet traffic in 2013. Websites targeted by scrapers may incur damages resulting from, among other things, increased bandwidth usage, network crashes, the need to employ anti-spam and filtering technology, user complaints, reputational damage, and costs of mitigation that may be incurred when scrapers spam users, or worse, steal their personal data.

Though sometimes difficult to combat, scraping is quite easy to perform. A simple online search will return a large number of scraping programs, both proprietary and open source, as well as D.I.Y. tutorials. Of course, scraping can be beneficial in some cases. Companies with limited resources may use scraping to access large amounts of data, spurring innovation and allowing such companies to identify and fill areas of consumer demand. For example, Mint.com reportedly used screen scraping to aggregate information from bank websites, which allowed users to track their spending and finances. Unfortunately, not all scrapers use their powers for good. In one case on which we previously reported, the operators of the website Jerk.com allegedly scraped personal information from Facebook to create profiles labeling people "Jerk" or "not a Jerk." According to the Federal Trade Commission (FTC), over 73 million victims, including children, were falsely told that they could revise their profiles by paying $30 to the website.

Website operators have asserted various claims against scrapers, including copyright claims, trespass to chattels claims and contract claims based on allegations that scrapers violated the websites' terms of use. This article, however, focuses on another tool that website operators have used to combat scraping: the federal Computer Fraud and Abuse Act (CFAA).

The CFAA was originally intended as an anti-hacking statute—and its application to scraping isn't always a foregone conclusion.

The CFAA imposes liability on "whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . " While the CFAA is primarily a criminal statute, it also provides for a civil remedy where a plaintiff suffers more than $5,000 in aggregate losses during any one-year period arising from a violation of the CFAA. For large website operators asserting CFAA claims against scrapers, the $5,000 damages requirement has not proven to be a difficult obstacle to overcome. For example, in *CollegeSource, Inc. v. AcademyOne, Inc.*, the District Court for the Eastern District of Pennsylvania found that the plaintiff's cost of initiating an internal investigation of the defendant's website, hiring a computer expert to analyze the scope of the defendant's actions and implementing increased security measures were well in excess of $5,000. Similarly, in *Facebook, Inc. v. Power Ventures, Inc.*, the District Court for the Northern District of California found that the plaintiff's expenditures made in response to defendant's specific acts, which included three to four days of engineering time, $75,000 in outside counsel costs and the costs of responding to a minimum of 60,000 instances of spamming by defendant, were well in excess of the statutory threshold. The more difficult question is whether scraping violates the CFAA at all.

The CFAA was originally intended as an anti-hacking statute and its application to scraping—which, after all, usually involves accessing publicly-available data on a publicly-available website—is not always a foregone conclusion. Does a scraper access a website "without authorization" or "exceed authorized access" when it harvests publicly-available data on a publicly-available website? Plaintiffs often argue that scrapers act without authorization because the websites' online terms of use prohibit scraping and/or prohibit the scrapers' use of the data that they harvest. As discussed below, such claims have met with success in some cases, but courts have been less willing to find a CFAA violation in other scraping cases.

In *Cvent, Inc. v. Eventbrite*, Cvent sued Eventbrite for scraping Cvent's website to obtain venue information and using the information in Eventbrite's "Venue Directory." Cvent claimed that this was a violation of the CFAA because Cvent's terms of use specifically stated that such activities were unauthorized. The District Court for the Eastern District of Virginia held that Eventbrite's actions did not constitute "hacking" in violation of the CFAA because the information was publicly available; Cvent's website did not require any login, password or other individualized grant of access; and Cvent's terms of use were difficult to locate. Therefore, the court granted Eventbrite's motion to dismiss, concluding that Eventbrite was authorized to access the information on Cvent's website, and that the mere allegation that Eventbrite used the information inappropriately was not grounds for relief under the CFAA.

Power Ventures, the defendant in *Facebook, Inc. v. Power Ventures, Inc.*, operated a social media account

BY THE NUMBERS

350 million people generated three billion World Cup posts, comments, and likes on Facebook[1]

World Cup-related Facebook interactions far exceeded interactions for the 2014 Super Bowl, Academy Awards and Sochi Winter Olympics combined[1]

The official FIFA app became the most popular sporting event app ever, with 28 million downloads[1]

The final World Cup match set a new Twitter record of **618,725 TWEETS PER MINUTE**[2]

MOST RETWEETED[3]
Tim Howard believes in the USA – 65,000
Rihanna supports Brazil – 32,000
Specsavers mocks Suarez's bite – 29,000

TOP BRAND HASHTAG[3]
1.1 million mentions of Adidas' #AllIn during the World Cup[3]

SOURCES

1. http://www.cnn.com/2014/07/14/tech/social-media/world-cup-social-media/
2. http://insidetv.ew.com/2014/07/14/world-cup-final-ratings-social-media/
3. http://blog.hootsuite.com/story-2014-world-cup-social-media-42-stats/

integration site. As part of a promotion to gain new members, Power Ventures provided users with a list of their Facebook friends, which Power Ventures obtained through scraping the Facebook website, and asked users to select friends to invite to use the Power Ventures site. Facebook notified Power Ventures that its access was unauthorized and blocked Power Ventures' IP addresses. However, Power Ventures' scraping technology was designed to circumvent such technological measures and the scraping continued. The District Court for the Northern District of California held that Power Ventures' accessing of Facebook was without authorization and violated the CFAA and accordingly, granted summary judgment to Facebook on the CFAA claim.

CollegeSource, the plaintiff in *CollegeSource, Inc. v. AcademyOne, Inc.*, maintained an archive of college course catalogs in PDF format and a hyperlink service called CataLink, both of which it made available to paying subscribers. AcademyOne, a CollegeSource subscriber, hired a third party to download college catalogs directly from college websites in order to compile a course description database. However, the third party instead copied some of the PDF documents from CollegeSource through CataLink. AcademyOne removed the CollegeSource documents from its system after receiving a cease and desist letter from CollegeSource, but CollegeSource nonetheless proceeded to bring a number of claims against AcademyOne, including CFAA claims based on the argument that AcademyOne accessed the documents without authorization and exceeded authorized access. The court held, however, that AcademyOne did not access the documents without authorization because those documents were available to the general public. CollegeSource's argument that AcademyOne exceeded authorized access was based on AcademyOne's alleged violation of CollegeSource's terms of use. The Court acknowledged that accessing a website in violation of the applicable terms of use has been held to support a CFAA claim in some cases, but was unconvinced by CollegeSource's argument here because CollegeSource's subscription agreement did not cover CataLink. Accordingly, the court granted summary judgment to AcademyOne on the CFAA claims.

In *Craigslist Inc. v. 3Taps Inc.*, 3Taps allegedly scraped Craigslist's website and republished Craigslist ads on its own site, craiggers.com. In response, Craigslist sent 3Taps a cease and desist letter revoking 3Taps's authorization to access Craigslist's website for any purpose, and reconfigured the website to block 3Taps. When 3Taps allegedly continued its scraping activities by using different IP addresses and proxy servers to conceal its identity, Craigslist brought suit under the CFAA. Even though Craigslist's website was publicly available, the District Court for the Northern District of California declined to grant 3Taps' motion to dismiss the CFAA claim. According to the court, while Craigslist may have granted the world permission to access its website, it retained the power

to revoke that permission on a case-by-case basis, a power it exercised when it sent the cease and desist letter and blocked 3Taps's IP addresses. Therefore, 3Taps's continued access was without authorization. The court also rejected 3Taps's attempt to invoke the Ninth Circuit's decision in *United States v. Nosal*. In *Nosal*, the Ninth Circuit had held that an employee's use of information in violation of an employer's policies did not constitute a CFAA violation where the employee's initial access to the employer's computer system was authorized. The court in 3Tap's concluded, however, that the "calculus is different where a user is altogether banned from accessing a website," as was the case with 3Taps.

Fidlar, the plaintiff in *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, provides its Laredo program to governmental agencies, such as county clerks' offices, which use Laredo to make public records available for viewing over the Internet. Laredo prevents users from downloading or electronically capturing the documents they view. Users who want a copy of a public record must pay the county a print fee. LPS, a real estate analytics company, contracted with many counties to access their public records using Laredo, but used a scraping program to capture documents electronically without paying any fees. Fidlar sued LPS for violating section 1030(a)(5)(A) of the CFAA, which imposes liability on anyone who " . . . knowingly causes the transmission of a program, code, or command, and as a result . . . intentionally causes damage without authorization, to a protected computer." The District Court for the Central District of Illinois denied LPS's motion to dismiss the CFAA claim, holding that Fidlar's complaint properly alleged that LPS undertook intentional actions that, among other elements of damage, compromised the integrity of Laredo.

In light of the cases discussed above, it seems that plaintiffs are likely to have more success asserting CFAA claims against scrapers where they clearly and unambiguously revoke authorization to access their websites and take affirmative steps to block the scrapers, as in *3Taps* and *Power Ventures*. In contrast, when the scraper ceases scraping after access is revoked and takes remedial action, as in *CollegeSource*, courts may be less willing to impose CFAA liability. As seen in *Cvent*, a mere terms of use violation, particularly where the scraper may not have actual notice of the terms of use, may not support a CFAA claim. Whether the scraper is simply using software to collect publicly available information more efficiently or to do something else—such as to avoid paying fees for the information, as seen in *Fidlar*—may also be relevant. In any event, in an era when data is expensive to collect, valuable to have and cheap to take, the CFAA, when properly used, remains a viable tool to combat scrapers.

GOOGLE GLASS INTO EUROPE: A SMALL STEP OR A GIANT LEAP?

By Susan McLean and Ann Bevitt

Google Glass ("Glass") is the most high profile of the new wearable technologies that commentators predict will transform how we live and work.

Until now, the Android-powered glasses were only available in the U.S. However, as of June 2014, Glass has been launched in the UK. Now, if you are 18 years old, have a UK credit card and address and a spare £1,000, you can purchase your own Glass and see what the fuss is all about.

Google has stated that it selected the UK for its second market because "[the UK] has a history of embracing technology, design and fashion and . . . there's a resurgence happening in technology in the UK." But perhaps it is also because the UK's data protection regulator, the Information Commissioner's Office (ICO), has a reputation for being one of the more pragmatic privacy regulators in Europe. Because, for all its exciting technological benefits, Glass raises some thorny legal issues, in particular in relation to privacy. In this alert we will address some of those key issues.

WHAT IS GOOGLE GLASS?

As many readers will already be aware, Glass is a form of wearable technology that gives its users hands-free access to a variety of smartphone features by attaching a highly compact head-mounted display system to a pair of specially designed eyeglass frames. The display system connects to a smartphone via Bluetooth. Glass can run specialized Android apps known as "Glassware." In its current form, Glass can pull information from the web, take photographs, record videos, make and receive phone calls (via the Bluetooth smartphone connection), send messages via email or SMS, notify its user about messages and upcoming events, and provide navigation directions via GPS. Although Glass is still in the testing stage and boasts only a modest set of features, the prototype device has already caused quite a stir. In particular, it has some triggered significant privacy concerns.

PRIVACY

In terms of privacy, Glass throws up a variety of issues. Due to its functionality, Glass is likely to process two types of data relating to individuals: (1) personal data and metadata relating to the wearer of the Glass ("Glass User") and (2) personal data and metadata relating to any member of the general public who may be photographed or recorded by the Glass User ("Public"). In June 2013, a group of regulators and the Article 29 Working Party, wrote to Google inviting Google to enter into a dialogue over the privacy issues relating to Glass. The letter pointed out that the authorities have long emphasised the importance of privacy by design, but added that most of the authorities had not been approached by Google to discuss privacy issues in detail. In Google's response, it stated that protecting the security and privacy of users was one of its top priorities. Google also identified various steps that it has taken to address privacy concerns, including a ban on facial-recognition Glassware.

PERSONAL DATA OF THE GLASS USER

As with any smartphone, Google will collect personal data and other metadata relating to each Glass User. Google will need to comply with its obligations under the UK's Data Protection Act 1998 (DPA). A key element of such compliance will be putting in place an appropriate privacy policy for Glass Users. However, to date, Google has encountered some difficulties in this regard.

Indeed, in July 2013, the ICO wrote to Google confirming that Google's updated privacy policy raised serious questions about its compliance with the DPA. In particular, the ICO believed that the updated policy did not provide sufficient information to enable UK users of Google's services to understand how their data will be used across all of the company's products. It stated that Google must amend its privacy policy, and failure to take necessary action would leave the company open to the possibility of formal enforcement action.

Google has argued consistently that its privacy policy complies with EU data protection law. To date, no formal action has been taken by the UK, although Google has faced action elsewhere in Europe (e.g., in Spain).

PERSONAL DATA OF THE PUBLIC

Glass Users who take photographs or video/audio footage of the Public in a recreational capacity will not be subject to the DPA because they can rely on the "domestic purposes" exemption. However, if Glass Users take photographs or footage for work purposes, their employers will need to ensure compliance with the DPA (see below).

Google states that Glass was designed with privacy in mind and argues that Glass poses no greater privacy risk to the Public than a smartphone with a built-in camera. However, critics point out that taking a photograph or video/audio footage with a smartphone is very different from taking a photograph or video footage with a more discreet wearable device like Glass. Further, the Bluetooth connection between Glass and the Glass User's smartphone allows the possibility of real-time facial recognition, which raises a more detailed set of privacy concerns for the person identified (for example, his/her identity and location will be logged by the technology provider in the form of metadata, whether he/she consents or not).

Google Glass has been launched in the UK, and just as in the U.S., the device continues to raise thorny legal issues, particularly in relation to privacy.

In response to these concerns, Google appears to be taking steps to implement changes to protect privacy. Google announced on June 3, 2013, that it would not allow applications with facial recognition on Glass. However, banning facial-recognition apps does not address the concern that people photographed or videoed by a Glass User, whether in a "zone of privacy" or in a public place in which there is no reasonable expectation of privacy, might not know what has happened. To deal with this point, Glass does limit a user's ability to take photos to cases where the Glass User either speaks an audible command or makes a visible swipe on the device's tactile sensor, and limits video recordings to ten seconds in length without a Glass User holding on to the tactile sensor.

Accordingly, as it is with smartphones today, we expect that the use of Glass in public spaces will need to be regulated via a combination of: (1) social norms; and (2) rules enforced by the businesses operating in those spaces. Indeed, in the U.S., various establishments (including restaurants, bars, cinemas and casinos) have, to date, banned the device from their premises, and it has been reported that certain UK cinemas, gyms and cafes are planning to implement rules about the wearing of Glass in their establishments. Google has itself published a guide for Glass users entitled *"How not to be a Glasshole."*

GLASS IN THE WORKPLACE: KEY ISSUES FOR COMPANIES

For some time commentators have identified a variety of potential uses for Glass in the workplace. The benefit of having access to information on a hands-free basis could be hugely advantageous to a variety of workers, including medical professionals and fire officers. There are also clear advantages for certain professionals, such as police officers and security guards, to be able to make contemporaneous recordings while on duty. But with Virgin Atlantic Upper Class staff recently conducting a trial use of Glass, its potential application in the workplace is far broader than you might initially anticipate.

Indeed, in June 2014 Google launched the first round of its "Glass at Work" programme, which is intended to encourage the development of Glassware in the form of enterprise applications. Its first partners include the provider of content for live broadcasts and context-aware applications for the sports, entertainment, building/security and medical industries; a provider of museum guides; and the provider of apps for the energy, manufacturing and health care sectors.

Any company implementing Glass at Work will need to ensure that it complies with its obligations under the DPA, in terms of the processing of personal data relating to both employees and third parties.

Note that, although there is currently no specific guidance from the ICO on

Glass (or any wearable tech, generally), in the wake of the introduction of Glass in the UK, the ICO has published a blog post identifying the potential data protection issues, titled, "Wearable technology – the future of privacy."

In its blog post, the ICO makes clear that organizations using wearable tech that capture video or pictures must address the issues identified in its revised CCTV code of practice. The revised code was launched by the ICO in draft form for consultation at the end of May 2014. The consultation concluded on July 1, 2014 and an updated version of guidance is expected to be published later this year. The ICO also refers in its blog post to useful guidance found in the Surveillance Camera Code of Practice. Although the code only applies to UK public authorities, other organizations are encouraged to follow the code and its guiding principles voluntarily.

The following are some of the key issues that an organization should take into consideration in respect of the use of Glass or the other new wearable technologies that are proliferating:

- Ensure data protection compliance:
  - carry out a privacy impact assessment to ascertain whether use of Glass is justified, necessary and proportionate, as opposed to less privacy-intrusive alternatives;
  - take a "privacy by design" approach. If Glass is identified as the most appropriate equipment for your purposes, ensure that its use is restricted so that it does no more than is necessary for its specified purpose;
  - establish who has responsibility for the control of information, e.g., deciding what is recorded, how the information should be used and to whom it may be disclosed;
  - ensure that appropriate privacy notices are provided to individuals who may be recorded to ensure that people are properly informed about how their details are being collected and used;
  - only collect information that is relevant, adequate and not excessive;
  - avoid using Glass to record audio, as this is unlikely to be justified;
  - delete information as soon as it is no longer required;
  - where any personal data collected via Glass is to be shared with third parties, ensure that appropriate contractual arrangements are put in place; and
  - regularly review whether use of Glass continues to be justified.
- Make all necessary adjustments to contractual documentation to take account of the use of Glass, including the collection of personal data and metadata via the device.
- Put in place policies that clarify when and where Glass can be worn and that prohibit covert recording, and carry out all necessary training on these. For example, as with smartphones, there may be some particularly sensitive buildings or locations where Glass is not permitted.
- Put in place appropriate technical security measures to protect the personal data and other sensitive information collected via Glass.
- Have in place appropriate procedures to wipe Glass if stolen or lost.
- Monitor use of Glass by employees and ensure that all Glass devices are returned prior to employees leaving the company.
- Take steps to ensure that confidential information and intellectual property is not compromised as a result of the use of Glass in the workplace.

CONCLUSION

The market for wearable tech has grown significantly in the last few months, and all the signs are indicating that it is going to keep on growing. Glass is just the next step in this market that now also boasts smart-watches, rings, brooches and other wearable devices. Google is testing the waters in the UK and, despite the significant concerns referred to above, it seems very likely that this "small step" from the U.S. to the UK is going to lead to a "giant leap" in the spread and take-up of wearable technology.

DRUGS AND THE INTERNET: FDA DISTRIBUTES NEW DRAFT GUIDANCE REGARDING SOCIAL MEDIA PLATFORMS AND PRESCRIPTION DRUGS

By Erin M. Bosman and Joanna L. Simon

On June 18, 2014, the Food and Drug Administration (FDA) promulgated two much-anticipated draft guidance documents on using social media to present information about prescription drugs and medical devices. The draft guidance documents, which were originally promised by the FDA in 2010, represent the FDA's latest attempt to provide direction for drug and device manufacturers concerning how and when they may use social media.

BACKGROUND

Drug and device labeling and promotion are highly regulated activities, subject to onerous approval requirements enforced by the FDA under the Federal Food, Drug, and Cosmetic Act (the "Act"). Under the Act, "labeling" includes "all labels and other written, printed, or graphic matter" that "accompany" a drug or device. 21 U.S.C. § 321(m); 21 C.F.R.

§ 1.3(a). This definition has been broadly interpreted by the courts to include materials that supplement or explain a drug or device, even when there is no physical attachment to the drug. *See Kordel v. United States*, 335 U.S. 345, 350 (1948).

The FDA's draft social media guidance represents the agency's latest attempt to provide direction for drug and device manufacturers concerning how and when they may use social media.

Rapidly growing Internet-based technologies have made it quicker and easier for both manufacturers and independent third parties to disseminate information about drugs and devices. This has led to a host of issues, including (1) what drug companies can say online about their drugs without violating the "misbranding" regulations; and (2) what drug companies can do with what third parties have said online about their drugs. The guidance documents attempt to answer both of these questions.

THE TWITTER GUIDANCE

"Internet/Social Media Platforms with Character Space Limitations – Presenting Risk and Benefit Information for Prescription Drugs and Medical Devices"

The FDA's position concerning manufacturers presenting "benefit information" for regulated drugs on electronic platforms with character space limitations is laid out in the Twitter Guidance. This Guidance instructs companies on the steps to take to avoid inadvertently "misbranding" a drug by providing information about a drug's benefits without disclosing accompanying risks. With that in mind, the Twitter Guidance provides the following direction for drug companies seeking to use space-limited social media platforms:

- Include the brand and established name, dosage form, and ingredient information;
- Ensure that any benefit information provided is accurate;
- Accompany benefit information with risk information;
- Provide direct access to a more complete discussion of the risks associated with the drug or device. Notably, the Twitter Guidance says the link should lead to a page devoted "*exclusively*" to risk information; and
- If both benefit and risk information cannot be communicated within the space limit, consider using a different platform.

To prove that it is not impossible to provide the required information within Twitter's 140 character limit (just very difficult), the Twitter Guidance provides the following — entirely fictional — example of an acceptable tweet:

> ***No Focus (remembrance HC1) for mild to moderate memory loss-May cause seizures in patients with a seizure disorder www.nofocus.com/risk*** *[134/140]*

Notably, this example from the FDA might not prove helpful in reality, especially considering that many drugs would be required to list more than one risk.

The main take-away from the Twitter Guidance is nothing new: to avoid enforcement, provide "truthful, accurate, non-misleading, and balanced product promotion." If a company cannot achieve this delicate balance within Twitter's space limitations, it should "reconsider using that platform for the intended promotional message."

THE MISINFORMATION GUIDANCE

"Internet/Social Media Platforms: Correcting Independent Third-Party Misinformation About Prescription Drugs and Medical Devices"

The Misinformation Guidance describes the "FDA's current thinking" about how manufacturers and distributors "should respond, if they choose to respond, to misinformation" related to FDA-approved products, specifically when the misinformation is disseminated by third parties over the Internet. Per the Guidance, "misinformation" is "positive or negative incorrect representations or implications" about a company's drug or device that is created by someone who "is not under the firm's control or influence." Thus, the Guidance does not apply when misinformation is created or disseminated by the firm itself.

Companies can, however, breathe a small sigh of relief; the Misinformation Guidance makes it clear that companies have no independent obligation to correct third-party posted misinformation. This may obviate the need for companies to continuously monitor and mine massive amounts of Internet data related to their products.

Nonetheless, the FDA recognizes that it may "benefit the public health" for companies to have the ability to correct misinformation about their products. With the public health benefit in mind, the Misinformation Guidance sets forth the following guidelines for companies that are seeking to voluntarily correct misinformation:

- Post the correction in the same area or forum where the misinformation is found. If that is not possible, reference the area where the misinformation can be found;
- Disclose that the person making the correction is a company employee;
- Include the package insert via PDF or link to the approved labeling;
- Limit the correction to the scope of the misinformation;

- Do not use the misinformation as a catalyst for promotional messaging; and
- Record misinformation corrections in case the FDA has questions or concerns.

The Misinformation Guidance's bottom line is that "if a firm voluntarily corrects misinformation in a truthful and non-misleading manner," then the "FDA does not intend to object if the corrective information . . . does not satisfy otherwise applicable regulatory requirements regarding labeling or advertising[.]"

CONCLUSION

Although the draft guidance documents provide some clarification on the FDA's positions, it is not clear that they provide a noticeable benefit to the industry. The strict requirements related to providing risk information, including linking to a page dedicated exclusively to risks, may sway companies away from using popular social media platforms at all. Indeed, the guidance documents may have the unintended consequence of limiting, as opposed to expanding, the information available to the public about a given drug.

Companies have until September 16, 2014, to submit comments on the draft guidance documents.

COURT HOLDS THAT DMCA SAFE HARBOR DOES NOT EXTEND TO INFRINGEMENT PRIOR TO DESIGNATION OF AGENT

By Lincoln Lo and Aaron Rubin

The safe harbor provisions in § 512(c) of the Digital Millennium Copyright Act (DMCA) provide a mechanism that insulates online service providers from monetary damages for infringing materials posted or stored by their users. To receive this protection, service providers must designate an agent to receive notice of claims of infringement with the Copyright Office and publicly post the agent's contact information on the website. A recent case in the Northern District of California, *Oppenheimer v. Allvoices, Inc.*, examined whether service providers can avail themselves of the § 512(c) safe harbor for infringing acts that precede designation of such an agent.

Allvoices is an online service provider that maintains a community-driven platform for the exchange of ideas as well as graphical, written, and audio content. Allvoices provides users with financial incentives to upload content to the site, and treats such users as "citizen journalists" and independent contractors. While it began providing access to contributor content in 2008, Allvoices did not designate its DMCA agent until March 2011.

The plaintiff, David Oppenheimer, is a professional photographer whose photographs were posted on Allvoices's website by contributors in January 2011. Oppenheimer learned that his photographs had been posted on the Allvoices website in February 2011, prior to Allvoices's DMCA agent designation. Oppenheimer sent a cease and desist letter to Allvoices in August 2011, several months after Allvoices designated its DMCA agent. While Allvoices eventually removed the photographs, Oppenheimer alleged that Allvoices failed to reply to his cease and desist letter and failed to terminate the accounts of repeat infringers, as required by the DMCA.

Allvoices argued that it was entitled to the protection of the § 512(c) safe harbor for all alleged infringements, not just infringement occurring after it had designated its DMCA agent. Allvoices did not cite any authority for this position, but maintained that, because the DMCA does not expressly carve out or preserve liability for pre-designation infringement, Congress had intended for the safe harbor to apply to such infringement.

The court rejected Allvoices's argument and held that, under the plain language of the DMCA, an online service provider may invoke the § 512(c) safe harbor only if it has registered a DMCA agent with the Copyright Office. According to the court, designation of an agent is a "predicate, express condition" for application of the safe harbors, so Allvoices could not avail itself of the safe harbors with respect to infringement that occurred prior to designation. The court cited two previous Northern District of California cases that came to similar conclusions, *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.* and *Nat'l Photo Group, LLC v. Allvoices, Inc.* (note that Allvoices was also a defendant in the latter case). On the merits, the court held that Oppenheimer sufficiently alleged claims of direct, contributory, and vicarious infringement to overcome Allvoices's motion to dismiss those claims.

Defendant Allvoices maintained that, because the DMCA does not expressly carve out or preserve liability for infringement before a DMCA agent is designated, Congress had intended for the safe harbor to apply to such infringement.

A question remains regarding the period of time during which Allvoices may be liable for infringement of Oppenheimer's photographs. Specifically, the court did not address whether Allvoices's potential

liability is limited to the period during which the photographs were posted on Allvoices's website prior to the date that Allvoices designated its DMCA agent with the Copyright Office. Regardless, the message is clear: online service providers should designate a DMCA agent with the Copyright Office as early as possible in order to obtain the protection of the applicable DMCA safe harbors.

SOCIAL MEDIA AND PROXY CONTESTS

By Enrico Granata and Jenny Wang

As the use of social media continues to grow, social media is likely to play an increasingly more prominent role in proxy contests. In this context, the recent Compliance and Disclosure Interpretations issued by the SEC's Division of Corporation Finance provide helpful clarifications on how social media outlets can be used in proxy contests in compliance with SEC regulations.

SOCIAL MEDIA'S IMPACT ON PROXY CONTESTS

Activist investors have used social media and have at times been able to "move the market" through social media statements in support of or against a public company. Carl Icahn first used Twitter to express his concerns against Dell Inc.'s buyout in 2013, referencing his interest in Dell in his first Twitter posting. Icahn also made extensive use of social media in the recent eBay, Inc proxy contest, in which Icahn pressured eBay to add two of Icahn's nominees to eBay's board of directors and to spin off eBay's PayPal division. Icahn made multiple statements related to the eBay proxy contest through his personal Twitter account, including a link to an article about eBay's corporate governance problems, links to letters on Icahn's website supporting his position and criticizing eBay, and short jabs at eBay that could stand alone within the 140-character limitation of a Tweet. Similarly, members of eBay's board also used Twitter to announce their positions against Icahn in the proxy contest (in April 2014, Icahn and eBay reached an agreement that put one of Icahn's nominees on the eBay board).

In the general effort to inform and persuade shareholders during a proxy contest, social media can be a powerful tool, and it can grab the attention of a larger audience. As Carl Icahn's example suggests, social media can be used to make statements with a length and tone tailored to a specific social media platform, and to share links to information and analysis that provide more depth and greater disclosure to an interested reader.

SEC GUIDANCE ON SOCIAL MEDIA USE IN PROXY CONTESTS

In April 2014, the SEC's Division of Corporation Finance issued new Compliance and Disclosure Interpretations to provide guidance on applying the SEC's rules regarding communications made under the Securities Act of 1933 (the "Securities Act") when statements are made utilizing social media channels. Under the Compliance and Disclosure Interpretations, the SEC addressed two concerns related to the use of social media in proxy contests: (1) the use of a hyperlink to information required by certain rules when a character-or text-limited social media platform like Twitter is used for communication or disclosure; and (2) a third party's re-transmission of a communication made by the company. Although the SEC has provided guidance on re-transmission of electronic communications made under Rule 134 and Rule 433 of the Securities Act, which apply to communications made by Carl Icahn, in connection with prospectuses, and did not specifically extend the guidance to Rule 14a-12 and proxy solicitations, we believe that the same principles under the Compliance and Disclosure Interpretations would apply to any re-transmissions of electronic communications made in connection with proxy contests under Rule 14a-12.

Rule 14a-12 under the Securities Exchange Act of 1934 requires that certain information, such as plain language disclosing a proxy contest participant's direct or indirect interests and a prominent legend advising investors to read the proxy statement, must be included in proxy contest solicitations and other regulated statements and communications to shareholders. Recognizing the growing use of social media, the SEC's Compliance and Disclosure Interpretations clarify that a hyperlink may be used to satisfy the legend requirements of Rule 14a-12 in limited circumstances when the digital communication is being made on an electronic platform that limits the length of one posting so the posting cannot fit both the statement and the required legend or other information together (Compliance and Disclosure Interpretations 110.01, 164.02, and 232.15), such as Twitter's limitation of 140 characters per post. Such required information must be linked through an active hyperlink that "prominently conveys, through introductory language or otherwise, that important or required information is provided through the hyperlink."

In the general effort to inform and persuade shareholders during a proxy contest, social media can be a powerful tool, and it can grab the attention of a wide audience.

The Compliance and Disclosure Interpretations also address the impact of a third party's re-transmission of statements or communications made by an issuer on social media platforms. The Compliance and Disclosure Interpretations clarify that an issuer that makes a regulated statement or communication on social media bears no responsibility for subsequent re-transmission of the issuer's statement

by a third party as long as they are unconnected (Compliance and Disclosure Interpretations 110.02 and 232.16.), meaning as long as the third party is not acting on behalf of the issuer and the issuer has no involvement in the third party's re-transmission of the issuer's statement.

Social media statements are given no less scrutiny than statements in other media. In thinking about how to use social media in a proxy contest, companies and investors should understand the SEC's requirements for statements and communications made through such platforms. For instance, the party issuing a statement through social media will still need to file solicitation materials with the SEC on the same day they are first used or disseminated. This does not change when the solicitation is contained in social media communication such as a Twitter post or hyperlinked information.

As for the new SEC guidance permitting the use of hyperlinked information, a question remains as to what presentations of a hyperlink will be deemed to qualify as prominently conveying that important or required information is provided through the hyperlink.

It can be expected that as the use of social media in proxy contests becomes increasingly more widespread and participants push the limits of social media communications, the SEC will offer additional guidance and clarification through additional Compliance and Disclosure Interpretations and published reports.

SUPREME COURT STIFLES AEREO, BUT TRIES TO KEEP THE CLOUD AWAY

By Craig Whitney and Whitney McCollum

In a closely watched case, the U.S. Supreme Court ruled in June 2014 in a 6-3 decision that Aereo's Internet streaming service engages in unauthorized public performances of broadcast television programs in violation of the Copyright Act, reversing the Second Circuit's decision in *American Broadcasting Companies, Inc. v. Aereo, Inc.* (No. 13-461).

In ruling against Aereo, the Court sought to limit its decision to Aereo's service—which the Court considered to be "equivalent" to that of a traditional cable company—and noted that it was not addressing the legality of cloud storage lockers, remote-storage DVRs and other emerging technologies. But the Court's interpretation of the public performance right in the context of Aereo's technology will nevertheless influence future decisions on whether the transmission of content using other technology constitutes copyright infringement.

BACKGROUND

Aereo provides broadcast television streaming and recording services to its subscribers, who can watch selected programing on various Internet-connected devices, including smart televisions, computers, mobile phones and tablets. Aereo provides its service through individual, "dime-sized" antennas that pick up local television broadcast signals and transmit those signals to an Aereo server where individual copies of programs embedded in such signals are created and saved to the directories of those subscribers who want to view such programs. A subscriber can then watch the selected program nearly live (subject to a brief time delay from the recording) or later from the recording. No two users share the same antenna at the same time, nor do any users share access to the same stored copy of a program.

In 2012, various broadcasting companies sued Aereo for copyright infringement in the Southern District of New York, claiming, among other things, that Aereo's transmission of the plaintiffs' copyrighted content to Aereo's subscribers violated the copyright owners' exclusive right to publicly perform those works. That public performance right, codified in the 1976 Copyright Act, includes (1) any performance at a place open to the public or any gathering with a substantial number of people outside the "normal circle of family and social acquaintances," and (2) the transmission of a performance to the public, whether or not those members of the public receive it in the same location and at the same time. This latter provision, commonly referred to as the "Transmit Clause," was added to the Copyright Act by Congress in part to overturn earlier Supreme Court decisions that had allowed cable companies to retransmit broadcast television signals without compensating copyright owners.

The district court denied the broadcast companies' preliminary injunction requests, finding that, based on Second Circuit precedent, Aereo's transmissions were unlikely to constitute public performances. The Second Circuit affirmed the decision, relying on that court's earlier decision in *Cartoon Network LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008) ("*Cablevision*"), which found that a cable company's remote-storage DVR system did not run afoul of the public performance right because each transmission emanated from a unique copy of a program that was sent only to an individual user. The Second Circuit held that Aereo does not engage in public performances because, as in *Cablevision*, Aereo's system makes unique copies of every recording, and each transmission of a program to a customer is generated from that customer's unique copy.

THE SUPREME COURT'S RULING

The Supreme Court addressed two questions regarding the public performance right: (1) Does Aereo "perform" a copyrighted work, and (2) Is that performance "public"? The answer to both questions, according to the Court, is yes.

Performance

The Court held that Aereo's service does "perform" audiovisual works under the Copyright Act's definition of that term, which is to "show [the audiovisual work's] images in any sequence or make the sounds accompanying it audible." According to the Court, under this definition, "*both* the broadcaster *and* the viewer of a television program 'perform.'" (Op. at 7.) The Court (contrary to the Second Circuit and the dissent) disagreed with Aereo's argument that it was simply a supplier of equipment that allows users to perform content, and that it did not itself perform such content. Instead, the Court determined that Aereo was essentially no different in substance than a traditional cable company, to which Congress expressly intended to have the public performance right apply.

The technological difference between Aereo and traditional cable systems at issue when the Transmit Clause was enacted—that the latter systems transmitted content constantly while Aereo's system remains inert until a subscriber indicates that she wants to watch a program—was insignificant to the Court. "Given Aereo's overwhelming likeness to the cable companies targeted by the 1976 amendments, this sole technological difference between Aereo and traditional cable companies does not make a critical difference here. . . . [T]he many similarities between Aereo and cable companies, considered in light of Congress' basic purposes in amending the Copyright Act, convince us that this difference is not critical here. We conclude that Aereo is not just an equipment supplier and that Aereo 'perform[s].'" (Op. at 10.)

Public

The Court also held that Aereo transmits its performance of the copyrighted works to the public. An entity transmits a performance if it "communicate[s] by any device or process whereby images or sounds are received beyond the place from which they are sent." (Op. at 11.) Although initially only an assumed definition for the purposes of evaluating Aereo's argument, the Court appeared to accept the definition that transmitting an audiovisual performance requires communicating "contemporaneously perceptible images and sounds of a work." Because Aereo's service satisfied this definition, the Court went on to note that the Transmit Clause of the Copyright Act contemplates that an entity can transmit a performance "through one or several transmissions, where the performance is of the same work." Accordingly, the Court concluded that "when an entity communicates the same contemporaneously perceptible images and sounds to multiple people, it transmits a performance to them regardless of the number of discrete communications it makes." (Op. at 14.)

The Court expressly dismissed concerns over how its Aereo decision will affect other areas of technology, and stated that it did not see this dispute as a cloud or remote storage case, but rather, a cable company "equivalent" situation.

That transmission is also public because Aereo communicates "the same contemporaneously perceptible images and sounds to a large number of people who are unrelated and unknown to each other." (Op. at 14.) Although not cited in the Court's opinion, a similar circumstance involving transmission of content to people who were "unrelated and unknown to each other" was found to be a public performance in *On Command Video Corp. v. Columbia Pictures Industries*, 777 F. Supp. 787 (N.D. Cal. 1991), which established that electronic delivery of a movie video tape signal to a single hotel room, pursuant to a system consisting of a computer program, a sophisticated electronic switch and a bank of video cassette players, was a public performance under the Copyright Act.

The fact that the Aereo service involves individual recordings for each subscriber that plays each recording only to its designated subscriber is, according to the Court, just the "behind-the-scenes way in which Aereo delivers television programming to its viewers' screens" but "do not render Aereo's commercial objectives any different from that of cable companies" or "significantly alter the viewing experience of Aereo's subscribers." (Op. at 12.)

Again the Court explained that Aereo was conceptually no different than a cable company. "In terms of the Act's purposes, these differences do not distinguish Aereo's system from cable systems, which do perform 'publicly.' Viewed in terms of Congress' regulatory objectives, why should any of these technological differences matter?" (Op. at 12.)

The Court ultimately held that: "Insofar as there are differences, those differences concern not the nature of the service that Aereo provides so much as the technological manner in which it provides the service. We conclude that those differences are not adequate to place Aereo's activities outside the scope of the Act." (Op. at 17.)

ATTEMPTS TO AVOID THE CLOUD

The Court expressly dismissed concerns over how its decision will affect other areas of technology, and stated that it did not see this dispute as a cloud or remote storage case, but rather, a cable company "equivalent" situation. (Op. at 16.)

Indeed, the Court specifically stated that it did not believe its "limited holding" would "discourage" or "control the emergence or use of different kinds of technologies." The Court even laid out areas that its decision did not reach, including "whether different kinds of providers in different contexts also

'perform'" and "whether the public performance right is infringed when the user of a service pays primarily for something other than the transmission of copyright works, such as the remote storage of content," and encouraged entities concerned about these areas to "seek action from Congress." (Op. at 16-17.) Notably, however, the Court *did* hold that "an entity that transmits a performance to individuals in their capacities as owners or possessors does *not* perform to 'the public'"—a seeming nod to the validity of cloud locker services (at least where users are storing authorized copies of works in their lockers). (Op. at 15.) Moreover, the Court stated that "[a]n entity does not transmit to the public if it does not transmit to a *substantial* number of people outside of a family and its social circle." (Op. at 15-16.)

Regardless, any evaluation of whether the transmission of content—whether by new or existing technology—violates the public performance right will have to be viewed under the language of the *Aereo* decision. For example, while the Second Circuit's *Cablevision* decision is not expressly overruled or even examined in the *Aereo* decision, any future determination as to whether remote-storage DVR technology violates the public performance right would likely first be analyzed under *Aereo*—not *Cablevision*, at least outside of the Second Circuit. And, within the Second Circuit, one envisions a lively, ongoing debate as to what extent *Cablevision* dealt with transmissions to individuals in their capacities as owners or possessors of the products at issue, which, as noted above, the Supreme Court viewed as a situation left unaffected by its *Aereo* ruling.

Finally, while Aereo's service was likened to a cable system, Aereo—and perhaps other technology comparable to Aereo's—is *not* a cable system under any other definition, including Section 111 of the Copyright Act governing secondary transmissions of broadcast programming by cable systems. Therefore, an open issue is what effect the *Aereo* decision will have on the future of these types of cable-esque services, such as Aereo, assuming they want to continue to operate, and particularly whether they will attempt to license from the copyright owners the content that these services seek to distribute.

WEBSITES HIT WITH DEMAND LETTERS ON ACCESSIBILITY ISSUES DESPITE COURTS' REJECTION OF CLAIM

By David McDowell

This year, numerous businesses have received letters asserting that their websites are not accessible to persons with disabilities, in violation of the Americans with Disabilities Act and California's Unruh Act. These letters threaten litigation and warn of large penalty claims under the Unruh Act. What these letters do not report is that California courts have repeatedly rejected claims that the ADA and the Unruh Act require accessible websites, including a recent dismissal order from Judge David Carter of the Central District of California.

In *Jancik v. Redbox*, plaintiff claimed that Redbox Digital's online streaming video service violated the law by not being accessible to deaf consumers. The court rejected the claim, finding that "Redbox Digital's website, which offers Redbox Instant, is not a 'place of public accommodation.'" (*Jancik*, Slip Op. at p. 11.) The court followed up by holding that Jancik's Unruh Act claims cannot proceed separately from his ADA claim. (*Id.* at p. 12.) This decision followed an earlier decision in *Cullen v. Netflix* dismissing ADA and Unruh Act claims on identical grounds.

In light of these decisions, website operators need not fall prey to demand letters threatening action without immediate payment of penalties and attorney's fees. Existing law does not support the claims.

California courts have repeatedly rejected claims that the Americans with Disabilities Act and California's Unruh Act require websites to be accessible to persons with disabilities.

While Ninth Circuit law does not presently allow a claim, website accessibility remains a hot topic among governmental regulators, disability access advocates, and plaintiffs' counsel. This June, the Department of Justice announced that long-delayed regulations phasing in standards for websites would be delayed until, at least March 2015. Those delays, however, have not prevented the law from evolving rapidly and applicable standards may be different outside California and the Ninth Circuit. Understanding where the law is and where it is likely to move will allow companies to make better decisions about their investments in websites and mobile applications. As one of the leaders in understanding and addressing accessibility issues in the digital world, we can help guide you through the complex and evolving landscape.

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**.