Volume 5, Issue 2, April 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

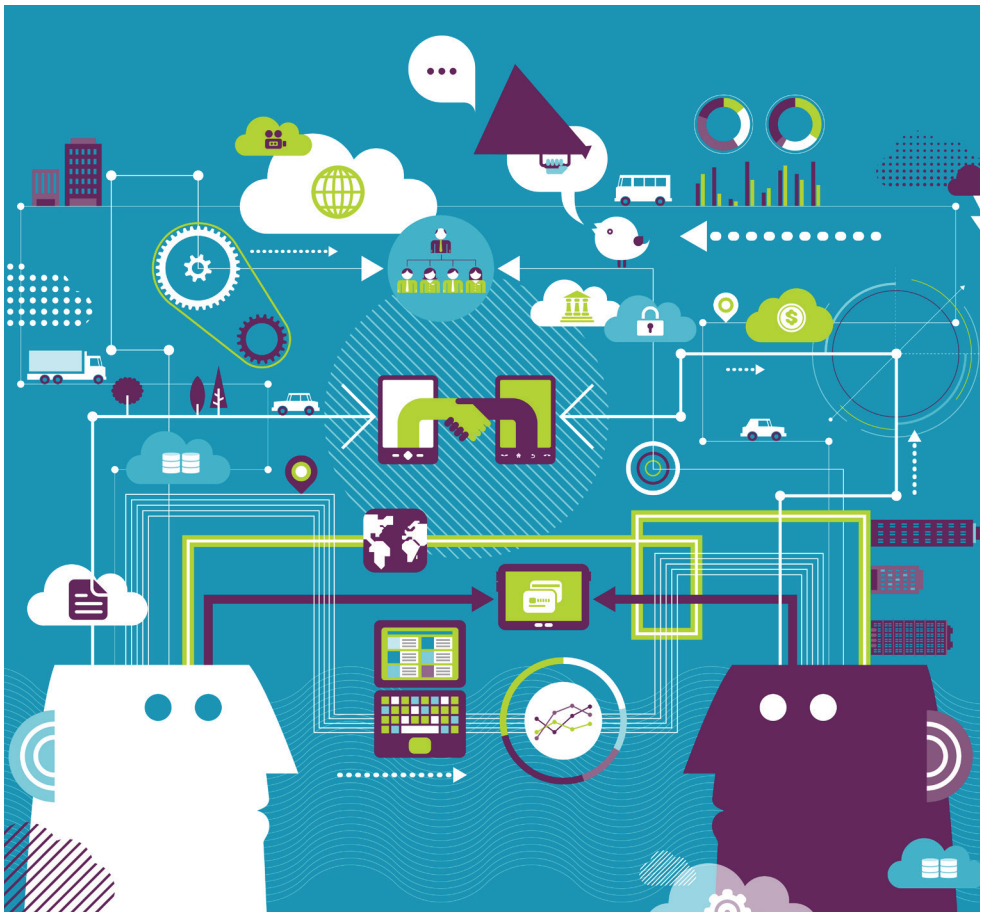
Reema Abdelhamid
Cindy Abramson
Chris Coulter
Melissa Crespo
Jacob Michael Kaufman
J. Alexander Lawrence
Christine E. Lyon
Gabriel E. Meister
Deirdre Moynihan
Aaron P. Rubin

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 summarize the current status of various state laws restricting employer access to the personal social media accounts of applicants and employees; we explore how driving while wearing Google Glass is butting up against the law, and examine recent attempts to legislate the use of Glass on the road; we report on various approaches U.S. courts are taking to address social media-related discovery challenges and to avoid social media fishing expeditions; we take a look at the legal landscape of so-called "revenge porn" and the laws victims are leveraging (or may be able to leverage in the future) in order to fight back; we discuss how UK and European copyright law is being applied to common Internet social and business practices, including the most basic of online activities—hyperlinking; and we highlight a puzzling recent Ninth Circuit decision that has operators of online video services and copyright experts alike scratching their respective heads.

All this—plus a collection of thought-provoking statistics about social media marketing...

EMPLOYER ACCESS TO EMPLOYEE SOCIAL MEDIA: APPLICANT SCREENING, 'FRIEND' REQUESTS AND WORKPLACE INVESTIGATIONS

By Melissa Crespo and Christine E. Lyon

A 2013 CareerBuilder survey of hiring managers and human resource professionals reports that more than two in five companies use social media to research job candidates. This interest in social media does not end when the candidate is hired: to the contrary, companies are seeking to leverage the personal social media of their existing employees, as well as to inspect personal social media in workplace investigations.

As employer social media practices continue to evolve, individuals and privacy advocacy groups have grown increasingly concerned about employers intruding upon applicants' or employees' privacy by viewing restricted access social media accounts. A dozen states already have passed special laws restricting employer access to personal social media accounts of applicants and employees ("state social media laws"), and similar legislation is pending in at least 28 states. Federal legislation is also under discussion.

These state social media laws restrict an employer's ability to access personal social media accounts of applicants or employees, to ask an employee to "friend" a supervisor or other employer representative, and to inspect employees' personal social media. They also have broader implications for common practices such as applicant screening and workplace investigations, as discussed below.

KEY RESTRICTIONS UNDER STATE SOCIAL MEDIA LAWS

As a general matter, these state social media laws bar employers from requiring or even "requesting" that an applicant or employee disclose the user name or password to his or her personal social media account. Some of these state laws also impose other express restrictions, such as prohibiting an employer from requiring or requesting that an applicant or employee:

- add an employee, supervisor or administrator to the friends or contacts list of his or her personal social media account;
- change privacy settings of his or her personal social media account;
- disclose information that allows access to or observation of his or her personal social media account, or otherwise grant access in any manner to his or her personal social media account;
- access personal social media in the employer's presence, or otherwise allow observation of his or her personal social media account; or
- divulge personal social media.

These laws also prohibit an employer from retaliating against, disciplining or discharging an employee or refusing to hire an applicant for failing to comply with a prohibited requirement or request.

Although these laws have the common goal of protecting employee privacy, their scope and terms vary, which creates a confusing landscape for multistate employers to navigate. Some of these laws only prohibit employers from seeking passwords or other login credentials to a personal social media account, while other states impose the broader restrictions described above. Certain states prohibit an employer from requiring an employee to change his or her privacy settings to allow the employer access to his or her private social media accounts, although it is possible that such a restriction might be inferred from at least some of the other state laws as well. Even more confusing are the inconsistencies across state laws with respect to exceptions for workplace investigations, as discussed below.

However, while state laws differ significantly, the general message is clear: employers must evaluate their current practices and policies to ensure compliance with these laws.

> Although state social media laws differ significantly, they have the common goal of protecting employee privacy—and the message is clear: employers must evaluate their current practices and policies to ensure compliance.

WHAT EVERY EMPLOYER SHOULD KNOW ABOUT STATE SOCIAL MEDIA LAWS

Applicant Screening

In general, these state social media laws do not limit an employer's ability to review public information, such as information that may be available to the general public on an applicant's social media pages. Instead, these laws limit an employer's attempts to gain access to the individual's social media accounts by means such as requesting login credentials, privacy setting changes or permission to view the accounts. Additionally, most of these laws explicitly state that they do not prohibit viewing information about an applicant that is available to the public, like information about an

BY THE NUMBERS
SOCIAL MEDIA MARKETING

Pinterest drives **twice** the website referral traffic of Twitter, LinkedIn and Google+ combined.[1]

Pinterest-referred shoppers are **10%** more likely to buy than Facebook-referred shoppers.[3]

25% of consumers who complain about products on Facebook or Twitter expect a response within one hour.[1]

52% of marketers say they have gained a customer via Facebook; **35%**, via Twitter.[2]

59% of marketers are using social media for six hours or more each week.[3]

87% of all small businesses say that social media helps their business.[2]

92% of companies that blogged multiple times a day have acquired a customer through their blog.[3]

SOURCES

1 http://www.spredfast.com/blog/2013/12/18/14-stats-to-inform-your-2014-social-marketing-strategy/

2 http://www.ziftsolutions.com/whats-new/infographic-social-media-root-modern-marketing/

3 http://www.hubspot.com/marketing-statistics

employee or applicant that can be obtained without any required access information or that is available in the public domain. However, all of these state social media laws prohibit employers from seeking access to the nonpublic social media pages of applicants. In practice, this means that employers should avoid asking applicants about the existence of personal social media accounts and requesting or even suggesting that an applicant friend the employer or a third party, including a company that provides applicant background investigations.

Friend Requests

Certain laws expressly restrict an employer's ability to encourage an employee to friend or add anyone to the list of contacts for his or her personal social media account. This may include the employer, its agents, supervisors or other employees. For example, Colorado's social media legislation states that an employer shall not "compel an employee or applicant to add anyone, including the employer or his or her agent, to the employee's or applicant's list of contacts associated with a social media account," and many other laws contain this type of prohibition against requesting access via what may be intended as a harmless friend request. Although these laws do not prohibit a subordinate from friending a manager or supervisor, employers should exercise care not to require, or even request or encourage, employees to friend supervisors or other company representatives. These restrictions may be particularly significant for employers seeking to leverage employees' personal social media connections for work-related marketing or business development purposes.

Employers should be aware that even in states without an express restriction on friend requests, a law that generally prohibits an employer from attempting to access an employee's or applicant's social media account may effectively limit an employer's ability to require or encourage employees to friend people. Even in states without social media laws or states with laws that allow "friending," employers should still proceed with caution when requesting access to an employee's or applicant's personal social media pages, and think twice about "friending" or "following" employees. If an employer learns about an employee's legally protected characteristic (such as religion, pregnancy or medical condition, or family medical history) or legally protected activity (such as political or labor union activity) by lawfully accessing the employee's social

media, the employer may face greater exposure to discrimination claims if it later takes adverse action against the employee.

Investigations

One of the most challenging areas under state social media laws involves an employer's ability to inspect or gain access to employees' personal social media in connection with workplace investigations. An employer may wish to access an employee's social media account, for example, if an employee complains of harassment or threats made by another employee on social media or if the employer receives a report that an employee is posting proprietary or confidential information or otherwise violating company policy. Some of the state social media laws provide at least limited exceptions for workplace investigations, while others do not.

- **No express exception for investigations:** The Illinois and Nevada social media laws do not provide any express exception for workplace investigations that might require access to an employee's personal social media accounts. This suggests that an employer's investigation of potential misconduct or legal violations may not justify requesting or requiring an employee to disclose his or her social media login credentials.
- **Limited exception for investigations of legal violations:** California's social media law provides that it does not limit an employer's ability to request that an employee divulge personal social media in connection with an investigation of employee violations of applicable laws. However, this exception does not appear to extend to other prohibited activities, such as asking an employee to disclose his or her user name and password for a personal social media account. Other states provide exceptions only for investigations of specific types of legal violations. For example, the Colorado and Maryland social media laws only provide an exception for investigating violations of securities laws or potential misappropriation of proprietary information.
- **Limited exception for misconduct investigations:** Some social media laws extend the exception beyond investigations of legal violations to investigations of alleged misconduct. These states include California, Oregon and Washington. In general, these laws allow an employer to ask an employee to divulge content from a personal social media account, but still do not allow the employer to request the employee's login credentials. In contrast, Arkansas permits an employer to request any employee's social media login credentials to investigate workplace misconduct.

Given these differences, employers should be mindful of the broad range of investigative exceptions in state social media laws. Before initiating an investigation that may benefit from or require access to an employee's personal social media, an employer should first consider the restrictions imposed by the applicable state law and the scope of any investigatory exception offered by that law.

Best Practices

Given the inconsistencies among the different laws, it is challenging for multi-state employers to manage compliance with all state social media laws. Even if it is not the employer's practice to seek access to its employees' or applicants' private social media pages, there are less obvious components of the laws that will affect almost every employer, and employers should consider the following measures:

- **Review hiring practices for compliance with social media laws:** Employers should ensure that all employees involved in the hiring process are aware of the restrictions imposed by these state social media laws. For example, recruiters and hiring managers should refrain from inquiring about an applicant's personal social media pages or requesting access to such pages. While these state social media laws do not prohibit employers from accessing publicly available personal social media sites, employers will also want to evaluate whether this practice is advisable, given the risk of stumbling across legally protected information that cannot be used in employment decisions.
- **Implement social media guidelines:** Employers should implement social media guidelines to mitigate potential risks posed by employee social media postings, being mindful of restrictions arising under the National Labor Relations Act and other federal and state laws. Employers also should ensure that their social media guidelines do not run afoul of these state social media laws.
- **Educate and train personnel:** Personnel involved in internal investigations, such as human resources and internal audit personnel, need to be aware of the growing restrictions on employer access to employee personal social media accounts. Prior to seeking access to an employee's personal social media account, or content from such an account, the internal investigators should check any applicable restrictions. In general, given the trends in these laws, employers should avoid requesting login credentials to employees' personal social media accounts, even in the investigation context, unless they have first consulted legal counsel.

DRIVING UNDER THE INFLUENCE (OF GOOGLE GLASS)

By Cindy Abramson and Gabriel Meister

In September 2013, *Socially Aware* took a close look at the potential legal issues confronting users of Google Glass, the now instantly recognizable, compact head-mounted display attached to a pair of specially designed eyeglass frames, which lets wearers access a variety of customized smartphone features.

In the meantime, Google's Glass Explorer Program has expanded steadily. In October 2013, the company announced the ability for each Explorer to invite three friends to join and purchase a Glass, and officially rolled out its "Glassware" app review program. With the expansion of the Glass Explorer Program, several of the issues we identified in the fall of 2013 have come into sharper focus, including one that could have a real impact on wearers' daily lives.

CALIFORNIA VEHICLE CODE SECTION 27602

On October 30, 2013, Cecilia Abadie was ticketed by a California police officer—not just for speeding, but for wearing her Google Glass while driving. The officer who ticketed Abadie cited a provision of California's Vehicle Code, VC Section 27602, for the Glass-related violation. The relevant portion of the law states:

> (a) A person shall not drive a motor vehicle if a television receiver, a video monitor, or a television or video screen, or any other similar means of visually displaying a television broadcast or video signal that produces entertainment or business applications, is operating and is located in the motor vehicle at a point forward of the back of the driver's seat, or is operating and the monitor, screen, or display is visible to the driver while driving the motor vehicle.

Naturally, VC Section 27602 was written before the advent of Google Glass (and it hasn't been amended since 2011). The law carves out several exceptions for equipment "when installed in a vehicle," including global positioning and mapping displays, rear-view cameras ("[a] visual display used to enhance or supplement the driver's view forward, behind, or to the sides of a motor vehicle for the purpose of maneuvering the vehicle"), and even television receivers that are disabled or unviewable while the vehicle is driven.

The story here is not uncommon. The law struggles to catch up with advanced technologies like Glass and other head-mounted displays; meanwhile, governments use old laws to address new risks, even though the fit isn't always perfect.

Abadie decided to fight the ticket, and on January 16, 2014, she was found not guilty by the San Diego Traffic Court Commissioner. You can read a copy of the ruling on Abadie's Google+ profile. The Commissioner's decision relied on the fact that there was no proof that Abadie's Glass was *in operation* while she was driving. This highlights an interesting difference between, on the one hand, dashboard-mounted screens, and on the other hand, compact head-mounted displays that may or may not have a visible "on" indicator: it's much easier for an onlooker (such as a police officer) to tell whether a dash-mounted screen is "operating" at any given time.

In November 2013—notably, after Abadie was issued her ticket—Google reportedly updated its Glass FAQ to answer the question, "*Can I use Glass while driving or bicycling?*":

> It depends on where you are and how you use it.
>
> As you probably know, most states have passed laws limiting the use of mobile devices while driving any motor vehicle, and most states post those rules on their department of motor vehicle websites. Read up and follow the law! Above all, even when you're following the law, don't hurt yourself or others by failing to pay attention to the road. The same goes for bicycling: whether or not any laws limit your use of Glass, always be careful.

SAFE DRIVING APPS ON GLASS

The question of whether driving while wearing Glass is legal is different from the question of whether it's safe. Many contend that Glass and similar devices simply add to an already long list of driver distractions. But others argue that some Glass apps—particularly apps that are specifically designed to be used while driving—are not only safe, but actually a positive alternative to using dashboard navigation systems that force drivers to take their eyes off the road repeatedly (and certainly a better alternative to the somehow irresistible urge to take out one's smartphone to check messages or hunt for traffic alerts). To put it another way, there's a difference between merely using Glass *while* driving, and using Glass *for* driving.

For example, one sideloadable Glass app, DriveSafe, is designed specifically to make driving safer by using Glass's built-in sensors to alert the driver when he or she appears to be nodding off. The app, which is activated with the phrase, "OK Glass, keep me awake," can even provide its wearer with directions to the nearest rest stop. Another developer, INRIX, is exploring the possibility of porting its traffic app to Glass in order

to enable drivers to receive real-time traffic alerts in their head-mounted displays and help them reroute their trips, all in a reportedly unobtrusive manner. Query whether the prevalence of safety-specific Glass apps will see the advent of a "driving mode" for wearable head-mounted displays.

There is at least one Glass app whose safety implications are tough to refute: developed by a firefighter in North Carolina, the app feeds critical emergency information, such as a fire's location and type, directly to a firefighter's line of vision while driving, potentially eliminating the need to reach for a radio, mobile phone, or other device to retrieve the same information. And firefighters may not be the only civil servants seeking to take advantage of Glass; in early February 2014, the NYPD announced that it is testing Glass for potential use by its officers. Although the specific uses being tested haven't been announced, it is easy to see how police officers could benefit from wearable head-mounted displays while driving, for example, by viewing details about crimes in progress, getting help with identifying vehicles, or recording offenders on the road.

THE FUTURE OF DRIVING WITH GLASS

Although it may be too early to accurately gauge the dangers of driving while wearing head-mounted displays, lawmakers are trying to regulate their use, and are likely to continue to do so—particularly where existing statutes might not do the trick. At least eight states are already considering bills that would regulate driving with Google Glass: Delaware, Illinois, Maryland, Missouri, New Jersey, New York, West Virginia, and Wyoming, whose proposed bill lumps Glass together with "texting while driving":

> No person shall operate a motor vehicle on a public street or highway while using a wearable computer with head mounted display, or while using a handheld electronic wireless communication device to write, send, or read a text-based communication.

And even though Glass is currently available only to U.S. residents (the Device Specific Addendum of Google's Glass Terms of Sale states, "You must be 18 years or older, a resident of the United States, and authorized by Google as part of the Glass Explorer program in order to purchase or use Glass Explorer Edition"), the UK government is already contemplating a ban on Glass for drivers.

It will be particularly interesting to see how these new pieces of legislation address drivers who wear corrective lenses. Originally, prescription lenses simply weren't compatible with Glass (although that didn't stop people from retrofitting earlier versions of the device with prescription lenses, including one man who was detained in January 2014 by federal agents after he wore his Glass to a movie theater and was suspected of trying to record the film using the device's camera). But in late January 2014, Google announced that it will be selling Glass frames that are designed to accommodate prescription lenses; and Vision Service Plan, the largest vision insurance provider in the United States, has announced that it will be offering subsidized frames and prescription lenses for Glass. As head-mounted devices with prescription lenses become more prevalent, we are likely to see a larger population of users who simply can't remove their head-mounted displays, particularly during vision-critical activities such as driving.

The story here is not an uncommon one. The law struggles to catch up with advanced technologies like Glass and their new perceived risks; meanwhile, governments continue to use old laws to address those new risks, even though the fit isn't always perfect. Keep your eyes on the road, and we'll keep our eyes on further Google Glass legal developments.

U.S. COURTS' EVOLVING APPROACHES TO SOCIAL MEDIA E-DISCOVERY

By Reema Abdelhamid and J. Alexander Lawrence

Courts across the United States have now made clear that discovery of social media is fair game. At the same time, courts have consistently found that litigants will not be permitted to engage in social media fishing expeditions; rather, litigants will be required to show that the sites likely contain relevant material. Below, we explore various approaches taken by courts to address social media-related discovery challenges.

Some courts have simply quashed a litigant's request for social media-related discovery for failure to show relevance to the dispute. In *Kennedy v. Contract Pharmacal Corp.*, the plaintiff sought a variety of gender discrimination-based damages. The defendants sought to compel broad discovery from the plaintiff's social media sites. For instance, the defendants broadly requested "[a]ll documents concerning, relating to, reflecting and/or regarding Plaintiff's utilization of social networking sites." Denying a motion to compel discovery, the U.S. District Court for the Eastern District of New York held that "[t]here is no specificity to the requests and no effort to limit these requests to any relevant acts alleged in this action."

In *Ford v. United States*, the U.S. District Court for the District of Maryland rejected the government's request for broad social media-related discovery. The government had sought "any documents[,] postings, pictures, messages[,] or entries of any kind on social media within the covered period relating to [c]laims by Plaintiffs or their [e]xperts." The court denied the motion to compel, holding that the

government's request was not narrowly tailored and "does not describe the categories of material sought; rather, it relies on Plaintiffs to determine what might be relevant."

Other courts, when quashing requests for social media-related discovery, have held that the litigants may renew a failed request, if circumstances change. For example, in *Root v. Balfour*, from Florida's Second District Court of Appeal, a mother had sued the City of Cape Coral, a construction contractor and a subcontractor for damages suffered by her son who was struck by an oncoming vehicle. The lower court had ordered the mother to produce various types of Facebook postings from both before and after the accident, including any information about counseling or psychological care she obtained; her relationships with her son and other children; and her relationships with other family members, boyfriends and significant others.

The appellate court quashed the order, finding that the requested discovery did not survive a relevance inquiry and that even the magistrate acknowledged that "95 percent, or 99 percent of this may not be relevant." The appellate court, however, held that if further developments in the litigation indicated that such information may be discoverable, the trial court might have to review information *in camera* and fashion appropriate limits regarding the discovery.

Other courts, while not quashing social media-related discovery requests entirely, have severely narrowed the requests before compelling production. For instance, in *Mailhoit v. Home Depot*, from the Central District of California, the defendant had demanded a wide array of social media-related discovery. These demands included (1) any profiles, postings or messages from social media sites relating to any mental state of the plaintiff; (2) third-party communications to the plaintiff that place her own communications in context; (3) any pictures of the plaintiff; and (4) social media communications between the plaintiff and current or former Home Depot employees or that in any way refer or pertain to her employment at Home Depot or the lawsuit. The court found the last category to be relevant and quashed the rest on the grounds they were not reasonably particular requests and therefore not likely to lead to discovery of admissible evidence.

Courts are taking various approaches to address social media-related discovery challenges and avoid social media fishing expeditions; we predict that these discovery issues will continue to arise, with even greater frequency.

In certain cases, courts have required the requesting litigant to show some information in the *public* social media profile that undermines the plaintiff's claim. In *Potts v. Dollar Tree Stores*, from the Middle District of Tennessee, the plaintiff sued for race-based employment discrimination, and the defendant requested, among other materials, full access to the plaintiff's Facebook page. The court found that the required showing had not been made. It concluded that the defendant "lack[ed] any evidentiary showing that Plaintiff's public Facebook profile contains information that will reasonably lead to discovery of admissible evidence."

We note, however, that at least one court has criticized the approach of looking to the *public* social media for indications of relevancy of the *private* portions of the site. In *Giacchetto v. Patchogue Medford Union Free School District*, the U.S. District Court for the Eastern District of New York observed that "[t]his approach can lead to results that are both too broad and too narrow" and went on to analyze category-by-category what the defendant had demanded to determine the scope of the relevant social media information in what the court called a "traditional relevance analysis."

Social media discovery has also sometimes involved the court itself reviewing documents in camera to determine relevancy. For example, in *EEOC v. Honeybaked Ham*, involving a hostile work environment class-action lawsuit, the U.S. District Court for the District of Colorado ordered that each class member's social media content be produced for review by the court in camera to determine what was legally relevant.

Similarly, in *Offenback v. Bowman*, from the Middle District of Pennsylvania, the plaintiff conceded that a limited amount of information in his Facebook account was subject to discovery, but the defendants argued for a much broader scope of discovery from the plaintiff. The court reviewed the information *in camera* and, siding with the plaintiff, determined that only a limited amount of information from the Facebook account had to be produced to the defendants.

Social media discovery issues will inevitably arise with even greater frequency in federal and state courts. As the courts struggle through the implications of such discovery issues, litigants should be aware that although social media is generally discoverable, courts are demanding more specificity in requests for social media information as they evaluate relevance.

KEEPING PRIVATES PRIVATE: THE LEGAL LANDSCAPE OF REVENGE PORN

By Jacob Michael Kaufman and Aaron Rubin

Mark Zuckerberg famously stated that the purpose of Facebook is "to make the world more open and connected," and indeed Facebook, other social media outlets and the Internet in general have brought worldwide openness and connection-through-sharing to levels unparalleled at any point in history. With this new universe of limitless dissemination often comes the stripping away of privacy, and "revenge porn," a relatively new but seemingly inevitable outgrowth of social media and the Internet, is stripping away privacy in the most literal sense.

Defining "revenge porn" is relatively simple and does not require any sort of "I know it when I see it" test; in short, "revenge porn" is the act of publicly disseminating nude photographs or videos of somebody without her or his consent. The name derives from the fact that the act is most often associated with spurned men posting photos on the Internet that were received from their ex-girlfriends in confidence, as "revenge" for breaking up with them or otherwise hurting them. But recently, more and more photos are popping up that either were taken without the victim's consent, or were obtained by hacking a victim's email or computer. Revenge porn website operators invite users to post nude photos of their exes (or of anybody else, for that matter) and often allow the community to comment on the photos (which in many cases results in a barrage of expletives aimed at shaming the victim).

Recently, operators of revenge porn sites have taken attacks to a higher level, inviting visitors to post victims' full names, addresses, phone numbers, places of work and other items of personal information alongside their photographs. In some cases, victims' faces are realistically superimposed onto nude photographs of pornographic actors or actresses in order to achieve the same effect when no actual nude photographs of the victims can be found. Victims of revenge porn often suffer significant harm, facing humiliation, loss of reputation, and in some cases, loss of employment. Due to the all-pervasive and permanent nature of the Internet, once a victim's photo is posted online, it is very difficult for him or her to have it completely removed. Operators of revenge porn sites have sometimes capitalized on this fact by offering to remove the photos for a fee (or running advertisements for services that will do so).

Operators of revenge porn websites often shield themselves behind the First Amendment, and website operators have been known to employ sophisticated legal teams in order to protect themselves from civil and criminal liability and to maintain operation of their sites. Nonetheless, the law provides several avenues for victims seeking to have photos removed from websites, obtain restitution and, to the extent damage has not already been done, clear their names.

SELF-HELP AS A FIRST STEP

Although the Internet is the tool used to disseminate revenge porn, it also now provides resources for victims who seek help in dealing with this invasion of privacy. The website WomenAgainstRevengePorn.com contains a step-by-step guide to getting nude photos removed from the Internet, as well as contact information for lawyers and other advocates for revenge porn victims in various states.

According to the site, the first step to mitigating the damage of revenge porn is to establish *more* of an online presence. Although this may be counterintuitive, it is actually a logical approach: one of the biggest harms of revenge porn is that a friend, family member or employer will find nude photos when entering the victim's name into a search engine. By opening Facebook, Twitter, Pinterest and Instagram accounts under his or her name, a victim may be able to move the revenge porn photo to a lower position in search engine results.

"Revenge porn" sites are stripping away privacy, but the law provides several avenues for victims seeking to have photos removed to obtain restitution and, to the extent damage has not already been done, clear their names.

Because nude photos tend to be spread quickly on the Internet, WomenAgainstRevengePorn.com also encourages victims to use Google's reverse image search engine to find all websites where the victim's photos may appear. After taking careful note of all locations where such photos appear, victims are encouraged to file police reports.

COPYRIGHT INFRINGEMENT

The next step recommended by WomenAgainstRevengePorn.com in removing photos, which has been successful in a number of cases (including as described in this particularly fascinating account), is for the victim to take advantage of U.S. copyright law. Under U.S. copyright law, a person who takes a nude photo of herself or himself is the owner of the copyright in that photo and thus can enjoin others from reproducing or displaying the photo. A victim may, therefore, submit a "takedown"

notice under Section 512 of the Digital Millennium Copyright Act (DMCA) to the webmasters and web hosts of the offending sites, as well as to search engine sites where the nude photo may come up as a search result (Google even provides step-by-step instructions). Because the DMCA provides an infringement safe harbor to web service providers who comply with the statute's requirements, many search engines and web hosts will remove revenge porn photos upon receipt of a takedown notice. If the photo is not removed, the victim may consider registering his or her copyrights in the photos and suing the web host or search engine in federal court, although this may not always be a desirable approach for the reasons described below.

Using copyright law to fight revenge porn, while effective to an extent, is not without problems, including the following:

- It only works if the victim owns the copyright. While many revenge porn photos are taken by the victim himself or herself and then posted without his or her consent, this is not always the case. In situations where another person took the photo—e.g., if the victim's girlfriend or boyfriend took it, or if the photo was taken secretly without the victim's consent—the victim would not be the copyright owner and thus could not use copyright law to force removal.
- Website operators may reject copyright infringement claims and refuse to remove the offending photos. Although a victim could move forward with litigation to obtain an injunction and possibly monetary damages, revenge porn operators are often confident that (a) the costs of litigation are too expensive for many revenge porn victims and (b) many revenge porn victims fear making their situations even more public by bringing suit. To mitigate the risk of such increased exposure, victims can attempt to bring suit pseudonymously, and there are resources on the Internet devoted to assisting with this.
- Even if a website operator removes the photos of one victim who follows all of the necessary steps to enforce his or her copyright, the website will still display photos of hundreds, if not thousands of other victims.

Thus, copyright law is not always enough to effectively combat revenge porn.

DEFAMATION, PRIVACY AND OTHER RELATED LAWS

Several victims of revenge porn, as well as people who have had other personal information of a sexual or otherwise inappropriate nature published on revenge porn websites, have launched civil lawsuits under theories such as defamation, invasion of privacy, and identity theft. As we have reported previously, one high profile example of this came in July 2013, when a federal judge in Kentucky allowed a defamation lawsuit against the operator of a site called TheDirty.com to proceed and a jury awarded the victim (about whom the site had published false accounts of her sexual history) $338,000.

Prosecutors have also taken advantage of the fact that the operators of these sites often engage in criminal activity in order to obtain and capitalize on nude photos. On January 23, 2014, Hunter Moore, known by some as the "most hated man on the Internet" and probably the most famous and successful revenge pornographer to date, was arrested on charges of illegally accessing personal email accounts in order to obtain photos for his revenge porn site. Further, California Attorney General Kamala Harris recently announced the arrest of a revenge porn site operator for 31 accounts of conspiracy, identify theft and extortion based on the unauthorized posting of nude photos. Depending on the outcome of these cases and civil cases such as that against TheDirty.com (and their inevitable appeals), revenge porn victims may soon have additional avenues of legal recourse.

The most commonly used defense of website operators against charges like those discussed above is 47 U.S. Code § 230(c)(1), the provision of the Communications Decency Act of 1996 (CDA) that states: "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Revenge porn website operators have cited this statutory provision to argue that they are not responsible for the images they host if the content was provided by other users. However, § 230 might not provide a defense in all cases. First, § 230 does not grant a website operator immunity from federal criminal laws, intellectual property laws or communications privacy laws (such as the laws that Hunter Moore allegedly violated). For example, if a website operator uses a photo of a victim submitted by a third party to extort money from the victim, § 230 would not provide any defense. Second, § 230 may not protect a website operator if the site contributes to the creation of the offending content. In the case against TheDirty.com referenced above, the court rejected the operator's § 230 defense, pointing out that the operator, who edited and added commentary to the submitted offending content, "did far more than just allow postings by others or engage in editorial or self-regulatory functions." It is noteworthy, however, that the website operator of TheDirty.com has filed an appeal in the Sixth Circuit and that TheDirty.com did prevail in a 2012 case based on similar facts.

STATE ANTI-REVENGE PORN LAWS

Another approach to deterring website operators from posting unauthorized nude photos is passing laws that criminalize that specific activity. As of today, only two states, New Jersey and California, have such laws. These laws are fairly limited in scope in order to pass constitutional muster under the First Amendment. California's law, enacted on October 1, 2013, is subject to a number of limitations. For example, it does not cover photos taken by the

victim himself or herself, it does not apply if a third party obtains the photos through hacking, and a website operator can only be prosecuted if the state can prove that the operator intended to cause emotional distress. Further, the penalties under this law are relatively minor: distribution of unauthorized nude images or videos is a misdemeanor, with convicted perpetrators facing six months in jail and a $1000 fine. Nonetheless, free speech advocates, including the Electronic Frontier Foundation (EFF), have criticized the law, stating that it is overly broad, criminalizes innocent behavior, and violates free speech rights.

Despite broad objections against anti-revenge porn laws from the EFF and various other free speech advocates, legislatures in several other states, including New York (where, in the absence of such a law, a state judge was recently forced to grudgingly acquit a revenge pornographer), Rhode Island, Maryland, and Virginia, have introduced laws that would criminalize operation of revenge porn websites. Further, the California Attorney General's office is currently prosecuting an Oklahoma-based revenge pornographer on the grounds that many of his victims resided in California, testing the reach of California's state statute. There is also discussion about enacting a federal anti-revenge porn statute. Whether these laws will be enacted, and the extent to which prosecutors will actually invoke these laws if they are passed, remains uncertain. But such laws could become powerful weapons in the fight to eliminate revenge porn.

As revenge porn is a worldwide phenomenon, jurisdictions outside the U.S. have also passed laws aimed at punishing the practice. For example, a law criminalizing non-consensual distribution of nude photographs of other people was passed in the Australian state of Victoria in December 2013. And, in January 2014, the Israeli parliament passed a law that criminalizes revenge porn, punishing website operators who publish unauthorized photos or videos of a sexual nature with up to five years in prison.

CONCLUSION

As long as people fall in (or out of) love (or lust) and cameras and the Internet exist, the proliferation of revenge porn websites will remain a troubling issue. As discussed above, however, the law does provide at least some recourse to the victims of revenge porn.

COPYRIGHT: EUROPE EXPLORES ITS BOUNDARIES (PART 1: LINK HUBS)

By Chris Coulter and Deirdre Moynihan

INTRODUCTION

This year, as the world celebrates the 25th anniversary of the World Wide Web, the Web's founder, Tim Berners-Lee, has called for a fundamental reappraisal of copyright law. By coincidence, this year we also anticipate a rash of UK and European legislative developments and court decisions centering on copyright and its application to the Web.

In our "Copyright: Europe Explores its Boundaries" series of articles—aimed at copyright owners, technology developers and digital philosophers alike—we will examine how UK and European copyright is coping with the Web and the novel social and business practices that it enables.

HYPERLINKING AND LINK HUBS

Everyone that uses the Web uses hyperlinks, and most of us may never consider whether we need permission to share a hyperlink with our friends and colleagues. As we know, hyperlinking is fundamental to the working of the Web.

However, content owners, such as film distributors, music companies, sports rights holders and owners of literary works, are deeply concerned that certain uses of this fundamental Web tool are exposing their copyright-protected works to damaging and unauthorized use. This is because the ability to hyperlink has led to the emergence of sites that host collections of hyperlinks to third-party content ("Link Hubs"). And many of these Link Hubs have achieved notoriety by providing access to precisely the kinds of content that rights holders are keen to protect (think Napster, think Megaupload…).

Perhaps surprisingly, until very recently it has been unclear whether using this fundamental Web facility to link to third-party content actually required the permission of the copyright owner of the linked content. A recent decision by the EU's highest court, the Court of Justice of the European Union (CJEU), has now clarified the position.

SVENSSON VS. RETRIEVER SVERIGE

In the high profile case of Case-466/12 *Svensson & Others v. Retriever Sverige AB* ("Svensson"), the CJEU was asked to decide whether Retriever Sverige, the operator of a Link Hub, had acted in breach of copyright law by providing links to news articles made freely available on the website of the Göteborgs-Posten newspaper. Svensson and other journalists said that Retriever Sverige's inclusion, on its website, of the link to their articles infringed their exclusive right to make the articles available to the public.

The question before the CJEU focused on whether or not the provision of a clickable link by Retriever Sverige constituted an act of "communication to the public" for the purposes of Article 3(1) of Directive 2001/29 (the "InfoSoc Directive"). Under that provision, authors have the "*exclusive right to authorize or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them*".

The CJEU broke the question into two parts:

- **Is linking an act of "communication of a work"?**

According to the CJEU, if a work is made available to the public in such a way that the public may access it, irrespective of whether the public in fact takes the opportunity to access that work, that is sufficient for there to be "an act of communication." The provision of clickable links to protected works amounts to the "making available" of those works and is therefore "an act of communication." So, this took Retriever Sverige's hyperlinks halfway to infringing copyright.

- **What is "the public"?**

The CJEU noted that the term "public" refers to an indeterminate number of potential recipients and that it implies a "fairly large number of recipients." According to the CJEU, the provision of links on a website aimed at all potential users of the website amounts to a communication to a particular public.

For Article 3(1) to apply, however, the question was whether the public to whom the link was communicated was (a) the same as the public to whom the original communication was made or (b) a "new public":

> "*a communication . . . concerning the same works as those covered by the initial communication and made, as in the case of the initial communication, on the Internet, and therefore by the same technical means, must also be directed at a new public, that is to say, at a public that was not taken into account by the copyright holders when they authorized the initial communication to the public.*"

Given that (i) the initial publication of the articles on the Göteborgs-Posten website consisted of a communication to all potential visitors to the website, and (ii) access to the articles on the Göteborgs-Posten website was not subject to any restrictive measures, the CJEU found that all Web users could, if desired, have free access to the articles on the Göteborgs-Posten website. Therefore, in the CJEU's opinion, the users of Retriever Sverige were deemed to be potential recipients of the initial Göteborgs-Posten communication; those users were a part of the same public taken into account by the journalists when they authorized the initial communication through Göteborgs-Posten.

The CJEU decided that hyperlinking on Retriever Sverige was not prohibited by Article 3(1) of the InfoSoc Directive and copyright infringement did not occur because Svensson and others had already permitted the relevant public to view the articles.

HYPERLINKING 1 – COPYRIGHT 0?

Superficially, this looks like a victory for linking over copyright. However, the CJEU's decision does not give blanket approval to all types of linking; for example, linking will not be authorised if it is communicated to a "new public." One way of determining whether there is communication to a new public will be if restrictions in place around the linked content (a pay wall, for example) have been circumvented by the Link Hub. This is because the new users via the Link Hub were not in the contemplation of the copyright holders when they authorised the original communication; so, in these circumstances the Link Hub would need the authorization of the copyright holder.

Based on this reasoning, it seems that, in Europe at least, linking designed to circumvent walled content restrictions, geographical restrictions or to restore access to deleted content is likely to amount to a communication to a "new public" and will require authorization. The key question is: what restrictions does a rights holder need to put in place in order to avoid its material being deemed to be freely available to the public? Is a paywall required or merely free subscription or registration? Is it possible to impose restrictions in a website's legal terms of use or access?

In addition, there seems to be direct application of the principle underlying the CJEU's Svensson decision to other forms of content that should be of interest to rights holders beyond news media.

In 2014 and beyond, we anticipate a rash of UK and European legislative developments and court decisions centering on copyright and its application to the Web, including "link hubs" and other novel Web-enabled social and business practices.

Of course, although the decision of the CJEU brings some clarity, there remains scope for creativity in the establishment of content protection "restrictions." However, for now this decision balances the legitimate interests of copyright holders with ongoing support for fundamental Web technology. So, we are calling a tie on this one, along with the observation that this is a good example of copyright adapting to, rather than being defeated by, the new digital landscape.

COMING NEXT…

In the *Svensson* case, the CJEU also appeared to endorse "content framing": it stated that its conclusion that linking is permitted where there is no "new public" is not altered if users of the link are given the impression that the work is appearing on the website on which the link is found when in fact it comes from another site.

Tantalizingly, the questions of linking and framing will be reviewed again by

the CJEU in *Case C-348/13 BestWater International and in Case C-279/13 C More Entertainment AB v. Sandberg*. It will be interesting to see how the CJEU applies its decision in Svensson in these and subsequent cases.

GOOGLE ORDERED TO REMOVE ALL COPIES OF ANTI-ISLAMIC FILM FROM YOUTUBE; DECISION PUZZLES COPYRIGHT ATTORNEYS

By J. Alexander Lawrence

An aspiring actress moves to California and finds her life threatened. While standard fare for pulp fiction, the case of *Garcia v. Google* involves a twist on this well-worn plot line that not even the most imaginative Hollywood scriptwriter could invent.

Cindy Lee Garcia answered a casting call for a low-budget amateur movie with the working title *Desert Warrior*. The film's writer and producer told her that it would be a "historical Arabian Desert adventure film." Ms. Garcia received $500 for her performance in the film. It turns out the actress was misled by the producer, Mark Basseley Youssef (aka Nakoula Basseley Nakoula, aka Sam Bacile), a Coptic Christian from Egypt, who was reportedly working in conjunction with an American non-profit, Media for Christ. The filmmakers had no intention of making an adventure film; rather, the end product—titled *Innocence of Muslims*—is an anti-Islamic account of the Prophet Mohammed that many Muslims find highly offensive and blasphemous.

In July 2012, Mr. Youssef posted a 14-minute trailer of the film to YouTube, which is owned and operated by Google. Ms. Garcia appears for about five seconds in the trailer. The film overdubs her voice with lines she never actually spoke. In September 2012, an Egyptian cleric issued a fatwa against all involved in the film, calling on Muslims to "kill the director, the producer, and the actors and everyone who helped and promoted the film." Ms. Garcia claims that she began to receive death threats and was forced to take precautionary measures at great expense to protect herself from retribution.

Sending takedown notices under the Digital Millennium Copyright Act, Ms. Garcia demanded that Google remove all copies of the trailer from YouTube. Google declined to do so. In September 2012, Ms. Garcia sued Google, also naming YouTube, asserting claims for copyright infringement. In October 2012, Ms. Garcia moved for a preliminary injunction, seeking to have Google take down all copies of the movie trailer from YouTube.

In November 2012, Judge Fitzgerald, a federal judge in Los Angeles, denied Ms. Garcia's motion. In a short opinion, Judge Fitzgerald held that Ms. Garcia was unlikely to be able to establish a copyright in her brief performance in the film. Judge Fitzgerald also found that her motion should be denied because of her delay in seeking the injunction after first seeing the film on YouTube and because of her failure to meet the heightened standard required to obtain a mandatory injunction in the Ninth Circuit.

Ms. Garcia appealed to the Ninth Circuit. On February 19, 2014, the Ninth Circuit issued a secret gag order—which was only later made public—directing Google to take down all copies of *Innocence of Muslims* from YouTube and any other platforms within its control and to take all reasonable steps to prevent further uploads. The court directed that neither the parties nor their counsel could reveal the existence of the order. The court later explained that it issued the secret gag order "to prevent a rush to copy and proliferate the film before Google can comply with the order."

On February 26, 2014, the Ninth Circuit released its opinion to the public. Two of the members of the three-judge panel sided with Ms. Garcia. The majority found that Ms. Garcia was in fact likely to prevail on her copyright claims and had established the other factors, such as irreparable harm, required to obtain a preliminary injunction.

In a lengthy dissent, Judge Smith expressed his strong disagreement with the majority's holding, complaining that "the majority abandons restraint to procure an end (order the film be taken down) by unsuitable means (the Copyright Act)." Judge Smith warns that "the majority makes new law in this circuit in order to reach the results it seeks." The Ninth Circuit, the circuit in question, is the home of Hollywood and its multibillion-dollar film industry.

In reaching his opinion, Judge Smith considered the bounds of copyright protection set forth in Section 102 of the Copyright Act, which limits copyright protection to "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." Judge Smith expressed his view that Ms. Garcia does not clearly have a copyright interest in her acting performance because (1) her acting performance is not a work; (2) she is not an author; and (3) her acting performance is too personal to be fixed.

As to the requirement that there be a protectable "work" at issue, Judge Smith considered the types of works that the Copyright Act lists as protectable, none of which include an acting performance. An acting performance is more akin to a procedure or process, which is specifically excluded from copyright protection, than an original work. Judge Smith noted that a motion picture is a "work," but the Copyright Act does not clearly place an acting performance within its sphere of copyrightable works.

As to the authorship requirement, Judge Smith looked to the Ninth Circuit's prior decision in *Aalmuhammed v. Lee*, in which an expert on the Spike Lee film *Malcolm X*, who suggested script revisions, directions to actors,

and help with the editing, claimed a copyright interest in the final work. The Ninth Circuit rejected his claim. Judge Smith found the majority's decision irreconcilable with *Aalmuhammed*. He noted that "[c]onsidering the number of contributors who inject the same or a greater amount of creativity into a film" when compared to Ms. Garcia's minor role, the majority's decision creates "an impenetrable thicket of copyright."

Copyright experts have expressed their puzzlement at the majority's legal analysis (and the court's secret gag order) in *Garcia v. Google*, and Google has now filed a petition seeking rehearing by the full Ninth Circuit.

As to the fixation requirement, Judge Smith looked to the Ninth Circuit's prior decision in *Midler v. Ford Motor Co.*, in which the popular singer and actress Bette Midler sued Ford for misappropriating her voice in a commercial. Ford had a license in the song and paid someone to mimic Ms. Midler's voice. The Ninth Circuit held that Ms. Midler's voice is not copyrightable. "The sounds are not 'fixed.' What is put forward . . . here is more personal than any work of authorship." Judge Smith recognized that Ninth Circuit precedent led to the conclusion that "just as the singing of a song is not copyrightable, while the entire song recording is copyrightable, the acting in a movie is not copyrightable, while the movie recording is copyrightable."

Finally, Judge Smith strongly disagreed with the majority's conclusion that to the extent Ms. Garcia's performance could qualify as a "work," it was not a "work for hire." Ms. Garcia did not enter into a written "work for hire" agreement. Nonetheless, such agreements are not required under the Copyright Act. The Copyright Act provides that a "work made for hire" is "a work prepared by an employee within the scope of his or her employment." Judge Smith noted that in determining whether an individual is acting as an employee, courts generally look to "the hiring party's right to control the manner and means by which the product is accomplished." In his view, all the evidence pointed to the filmmakers' complete control over Ms. Garcia's work.

Copyright experts have expressed their puzzlement at the majority's legal analysis. In his widely followed blog, law professor Eric Goldman complained that the decision "is so terrible that there's simply no point trying to make sense of it."

On February 27, 2014, a day after the issuance of the opinion, YouTube filed an emergency motion for a stay pending the disposition of a petition for review by the full Ninth Circuit. YouTube warned that "[u]nder the panel's rule, minor players in everything from Hollywood films to home videos can wrest control of those works from their creators, and service providers like YouTube will lack the ability to determine who has a valid copyright."

The next day, the court denied that motion but modified its order to provide that it "does not preclude the posting or display of any version of 'Innocence of Muslims' that does not include Cindy Lee Garcia's performance."

Clicking on a link to the *Innocence of Muslims* on YouTube results in the following disclaimer: "This video is no longer available due to a copyright claim by an actress over her 5-second appearance in the video. A U.S. court has ordered Google to remove the video. We strongly disagree with this copyright ruling and will fight it. Sorry about that." Of course, the Internet being the Internet, the film is available on other sites.

It turns out that the film has also apparently still been popping up on YouTube from time to time. On March 25, 2014, Ms. Garcia moved for sanctions against Google, claiming it failed to stop users from uploading the film to YouTube. Ms. Garcia also complains that Google continues to publish links on its search engine to other sites where the video is available for viewing or download. Ms. Garcia accuses Google of "thumbing its nose at the Court" and seeks hundreds of thousands of dollars in sanctions. In response to the motion, Google outlined its extensive efforts, through both automated and manual processes, to identify the film among the hundreds of millions of videos on YouTube and to block access to newly uploaded copies. Google further noted that it had no obligation under the order to remove search engine links to the film on third party sites. The Ninth Circuit promptly denied Ms. Garcia's motion.

No one could fail to be sympathetic to Ms. Garcia's situation. Tricked into participating in the production of a hate film, her life has been turned upside down. The Ninth Circuit's decision, however, strains to find a legal justification for the court's desired outcome. As other commentators have noted, this appears to be a case of bad facts making bad law.

The Ninth Circuit panel may not have the last word here. Google has filed a petition seeking rehearing by the full Ninth Circuit. Ms. Garcia's opposition to Google's petition is due in early April, and other interested parties will have the right to submit friend of court briefs shortly after Ms. Garcia files her opposition. Facebook, Pinterest, Twitter, IAC/InterActiveCorp, the *Los Angeles Times*, the *New York Times* and the *Washington Post* have all expressed their intention to weigh in. We will see whether the full Ninth Circuit agrees to review the panel decision.

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**.