Morrison & Foerster Social Media Newsletter

Vol. 3, Issue 4 August 2012

Socially Aware:

The Social Media Law Update

2011 Best Law Firm Newsletter

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION

In this issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media, we explore whether one can serve legal notice through Facebook and other social media platforms; examine the ongoing dispute between Twitter and the Manhattan District Attorney over the discovery of user tweets; summarize the NLRB's latest guidance regarding workplace social media policies; review a controversial provision from Amazon Web Services's customer agreement; take a look at a putative class action lawsuit against the Pittsburgh Penguins hockey team arising out of the team's text messaging activities; highlight regulatory challenges to broker-dealers and investment advisers in using social media; visit a recent fair use decision in connection with a *South Park* parody of a viral video; and discuss the California Attorney General's formation of a new Privacy Enforcement and Protection Unit. All this plus our statistical snapshots showing the growing popularity of mobile devices (and the corresponding decline of PCs).

Follow us on Twitter @MoFoSocMedia, and check out our blog.

IN THIS ISSUE

"You Have One New Lawsuit": Can You Serve Legal Notice Through Social Media?

Can a litigant be served via social media? On June 7, 2012, in *Fortunato v. Chase Bank*, a federal district court ruled that defendant Chase Bank could not use Facebook to serve a third-party defendant with the complaint that Chase had filed against her.

In *Fortunato,* plaintiff Lorri Fortunato sued Chase Bank, alleging that the defendant had unlawfully garnished her wages to pay a credit card debt that, according to the plaintiff, was actually incurred by her estranged daughter, Nicole (who the plaintiff alleged had lied on a credit card application in order to open an account in her mother's name). Chase sought to implead Nicole in the matter, but was having a difficult time physically locating her; indeed, as the court noted, Nicole apparently had a "history of providing fictional or out of date addresses[.]"

Chase hired a private investigator, who "searched . . . [Department of Motor Vehicles] records, voter registration records, . . . Department of Corrections records, publicly available wireless phone provider records, and social media websites" for a way to contact Nicole. The private investigator's search turned up four possible addresses for Nicole in four different towns, but the defendant remained unable to physically locate her at any of those locations.

The private investigator did, however, find what she believed to be Nicole's Facebook profile, which listed a contact email address and a location in yet a *fifth* town. In view of this discovery, and given that Chase's "numerous attempts to effect personal service" and "diligen[t] . . . search for an alternate residence where Nicole might be served" had not succeeded, the bank suggested a novel alternative to the court: serving Nicole with notice by sending her a message on Facebook.

Chase argued that service through Facebook would meet due process requirements because it was "reasonably calculated to apprise" Nicole of the claims against her (echoing the words of the U.S. Supreme Court in *Mullane v. Central Hanover Bank & Trust Co.)*, and that it should therefore be an acceptable alternative means of service. Although the court agreed as an initial matter that some form of alternative service would be appropriate, the court rejected Chase's argument, ruling that service by Facebook would not be sufficiently "reasonably calculated to apprise" Nicole under the circumstances. Noting that "anyone can make a Facebook profile using real, fake, or incomplete information," the court found that "[Chase] ha[d] not set forth any facts that would give . . . a [sufficient] degree of certainty that the Facebook profile . . . [was] in fact maintained by Nicole[.]" The court then ordered Chase to publish notifications in the local newspapers for all five towns that its private investigator had identified as possible residences for Nicole.

The *Fortunato* court prefaced its analysis by remarking that "[s]ervice by Facebook is unorthodox to say the least," and that the court was "unaware of any other court that ha[d] authorized such service." But, as it turns out, at least a handful of courts—in the United States and abroad—appear to have done just that. In May 2011, a local state court in Minnesota permitted service of a petition for divorce by Facebook (or, indeed, "[any] other social networking site"), finding that, compared to the "antiquated . . . and prohibitively expensive" traditional means of publishing notifications in local newspapers, service through social media would be both cheaper and more likely to actually reach the party at issue. (And, although not a ruling on the issue, official form documents on the Utah State Court system's website can be read to suggest the use of Facebook and Twitter as possible alternative means of service.)

Outside of the United States, several courts—including courts in New Zealand, Australia, Canada and the United Kingdom—have affirmed or even endorsed the use of Facebook and other social media sites as acceptable alternative means of serving counterparties with notice of the claims brought against them.

The *Fortunato* court's approach does not necessarily contradict these examples, given that the *Fortunato* court did not categorically reject service by Facebook or other social networks. Rather, the court concluded that service through Facebook would not be appropriate under the circumstances of the case at issue. Which begs the question: what might the right circumstances be?

As a general matter, the law still favors traditional personal service as its preferred and primary method—the often-depicted "you've been served" moment of physically handing a summons and complaint to a party to be served. Statutes in U.S. jurisdictions also typically expressly authorize other traditional means of service, for example, delivery to a party's residence or agent. When these methods prove impractical, statutes typically authorize courts to allow some sort of appropriate alternative means of service. But in a case like *Fortunato,* assuming that the complainant has demonstrated that alternative service should be permitted, what might need to be shown in order to demonstrate to the court's satisfaction that service through social media would be appropriate?

The *Fortunato* court expressly identified a first major hurdle, which some have termed "authentication." In order to demonstrate a reasonable likelihood that the counterparty is actually going to receive notice, the complainant needs to be able to convince the court that the social media profile in question really does belong to the party to be served, and is not under the control of a different person with the same or a similar name (or even, perhaps, an impersonator). This has some parallels to the issues

Service through social media and other Internet-based means of communication could become a viable alternative to personal service, given that electronic service may have certain distinct advantages over the traditional means of alternative service used where no physical address is available.

raised when trying to use social media evidence in the context of a trial.

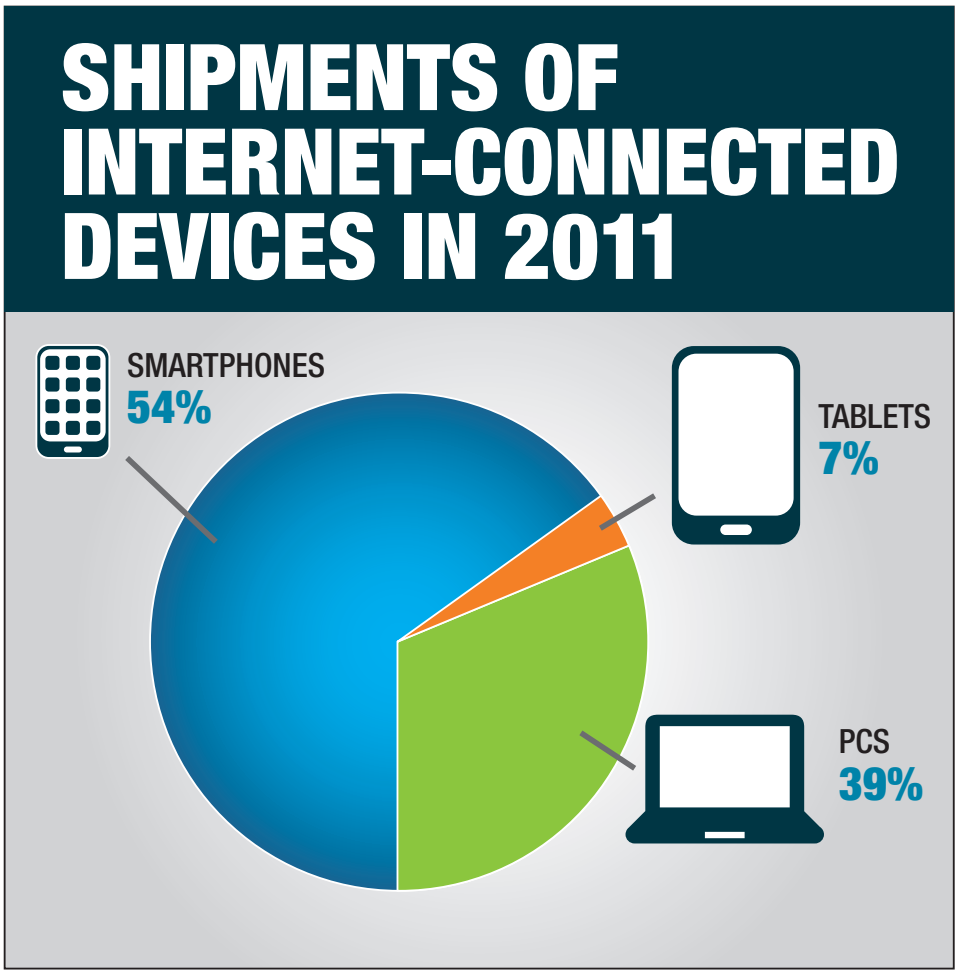
A second hurdle, somewhat less explicit in the *Fortunato* court's ruling, is whether—even if the social media profile *does* belong to the party to be served—the profile's owner regularly (or ever) logs in to or checks that profile. Being able to demonstrate this fact could help support an argument that "the person to be served would be likely to receive the summons and complaint" through his or her social media profile, which, as the *Fortunato* court noted, was important in cases where service by email has been accepted.

Cases from various countries, coupled with some creative thinking, provide helpful guidance for how a party that wants to serve notice through social media could surmount the hurdles above. For example, a party could try to demonstrate:

- That the personal biographical details listed in the profile match the party to be served's basic personal information (e.g., date of birth, educational history and/or work history);
- That recent photos of the party to be served have been posted to the profile;
- That the profile's "friend" or contact list corresponds with the party to be served's known real-world acquaintances;
- That updates, posts and other interactions on the profile's "wall" identify the user as the party to be served;
- That the profile's user has responded to recent friend requests, wall posts or private messages; and
- That third-party testimony corroborates the assertion that the profile belongs to the party being served.

Depending on the applicable social media profile's privacy settings, much of this information may be readily accessible to the general public. (Yes, people do still leave their social media profiles wide open.) Of course, practitioners should keep in mind ethical rules when using social media to obtain information.

In the long run, service through social media and other Internet-based means of communication could become a viable alternative to personal service, given that electronic service may have certain distinct advantages over the traditional means of alternative service used where no physical address is available (i.e., publication in local newspapers and posting of public notices). First, as noted in the Minnesota case described above, electronic notice can be far quicker, cheaper and easier. Second, as the Minnesota court also noted, notice may actually be more



Source: http://www.idc.com/getdoc.jsp?containerId=prUS23398412

likely to *reach* the intended recipient if delivered through social media than if communicated through those more traditional means. And third, some means of Internet communication enable senders to confirm electronically that their messages have been opened or received by the intended recipients.

Given the likelihood that attempted service through social media will be around for a while, we look forward to keeping you posted on future developments.

We've Come for Your Tweets: Twitter to Appeal Denial of Its Motion to Quash District Attorney's Subpoena

As the Occupy Wall Street protests fade from memory, a related discovery battle between Twitter and the New York County District Attorney rages on.

Earlier this year, we discussed the District Attorney's efforts to subpoena user information and tweets of criminal defendant Malcolm Harris, an Occupy Wall Street protester charged with disorderly conduct for allegedly occupying the roadway of the Brooklyn Bridge. In a setback for Twitter, the Criminal Court of the City of New York recently denied Twitter's motion to quash the District Attorney's subpoena; Twitter has announced its decision to appeal the court's decision. In this article, we take a look at the court's decision rejecting Twitter's motion, and discuss key issues to be addressed on appeal.

As noted, the dispute emerges from the District Attorney's criminal prosecution of Harris. Believing that Harris had tweeted information inconsistent with his anticipated defense, the District Attorney sought from Twitter the user information and tweets associated with the account @destructuremal—the Twitter account allegedly used by Harris. Harris filed a motion to quash, and Twitter refused to comply with the subpoena pending the results of Harris's motion.

The court found that Harris lacked standing to quash the third-party subpoena on Twitter, because Harris had neither a proprietary interest nor a privacy interest in the user information or tweets associated with the @destructuremal account. The court observed that no search warrant was required to obtain Harris's tweets, as no Fourth Amendment privacy rights are implicated when information is sought from a third party, such as Twitter. Rather, in a criminal case, the Stored Communications Act (SCA) permits the government to subpoena subscriber and session information directly from a social media site. The court ordered Twitter to comply with the subpoena.

Twitter then filed its own motion to quash the subpoena. Twitter argued that, under its Terms of Service, Harris in fact retained his rights to any content that he submitted, posted or displayed on or through the Twitter service; and that denying Harris's standing to oppose the subpoena placed an undue burden on Twitter. In a decision handed down on June 30, 2012, the court disagreed. The court noted that the general rule in New York is that "only the recipient of a subpoena in a criminal case has standing to quash it," and reiterated that Harris had no Fourth Amendment privacy right in his tweets. Twitter has objected to the court's decision, and, as noted, will be filing an appeal; a review of the court's decision highlights key issues to be addressed on appeal.

No Privacy Violation

Proving a violation of the Fourth Amendment requires a showing of either (1) a physical intrusion onto personal property or (2) a violation of a reasonable expectation of privacy. The court found that, due to Harris's publication of his tweets to third parties, neither showing could be made here.

With regard to any expectation of privacy, the court likened posting a tweet to screaming out of an open window.

No Physical Intrusion

With regard to physical intrusion, the court stated simply that there had been no physical intrusion into Harris's Twitter account. Unlike the contents of someone's home or car, the contents of Harris's Twitter account had been "purposely broadcast to the entire world [and] into a server 3,000 miles away."

No Reasonable Expectation of Privacy

With regard to any expectation of privacy, the court likened posting a tweet to screaming out of an open window. According to the court, "If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world." The court distinguished a tweet, however, from a "private" Internet dialogue, such as one conducted via private email, private direct message, or private chat. Accessing relevant information from such private Internet dialogues "would require a warrant based on probable cause." A tweet, however, is not like an email sent to a single party, and "[t]here can be no reasonable expectation of privacy in a tweet sent around the world."

A Tweet Is a "Public Posting"

The court based its decision on its finding that a tweet is a "public posting." In the court's view, "It is the act of tweeting or disseminating communications to the public that controls." The court supported its finding by citing Twitter's Privacy Policy, which states that "[o]ur Services are primarily designed to help you share information with the world. Most of the

information you provide us is information you are asking us to make public." As further evidence of the public nature of a tweet, the court also cited Twitter's 2010 agreement with the Library of Congress, under which every public tweet since Twitter's inception is to be archived; several Internet sites through which deleted tweets remain accessible; and a National Geographic Channel project that has collected tweets and intends to broadcast them into space this August.

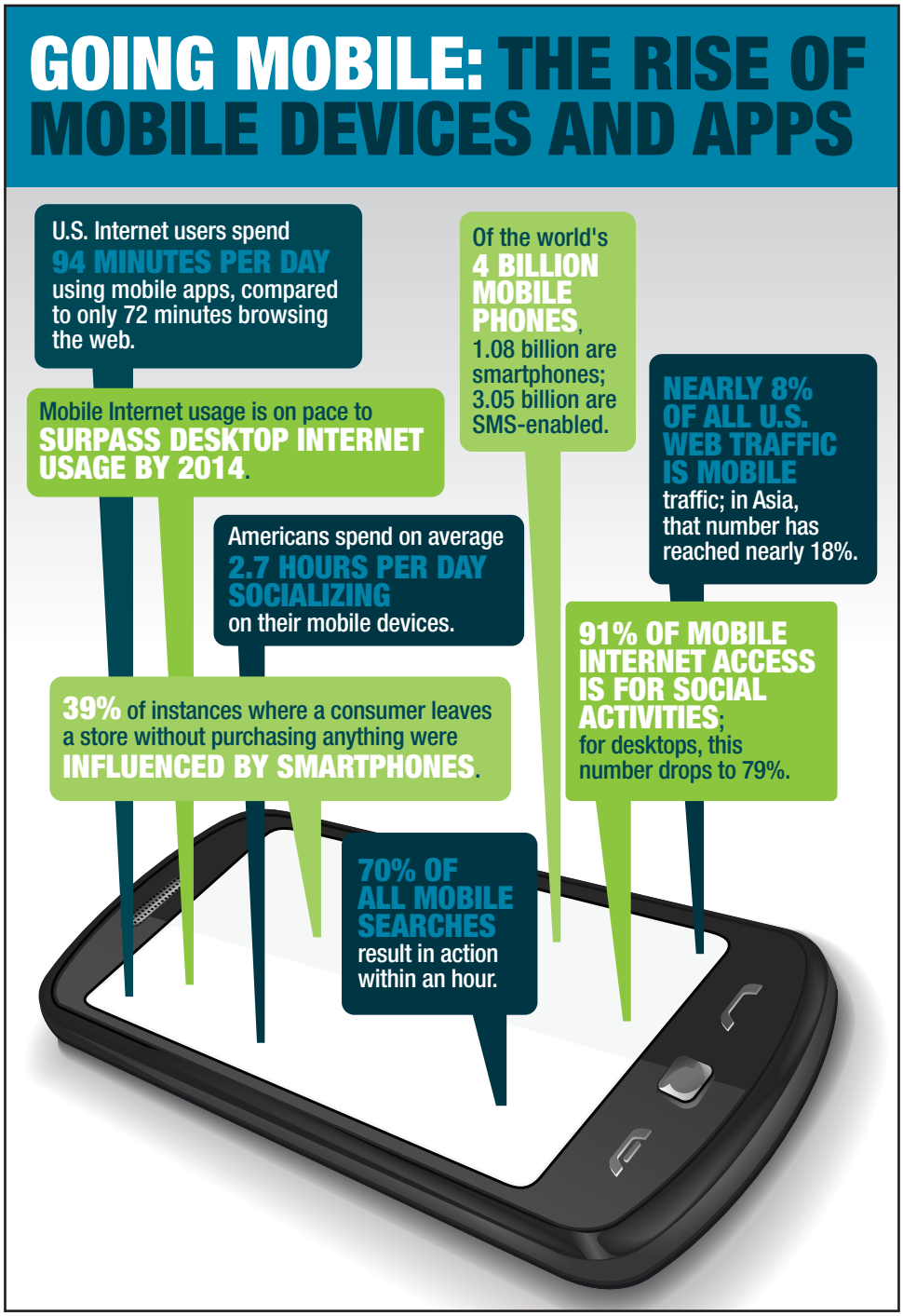
The court likened the third-party recipient of a tweet to a witness on the street who overhears something screamed out of an open window. As the court put it, "today, the street is an online, information superhighway, and the witness can be the third party providers like Twitter, Facebook, Instagram, Pinterest, or the next hot social media application." A tweet, like a scream out the window, has been made public, and "[t]here is no reasonable expectation of privacy for tweets that the user has made public."

No Undue Burden on Twitter

Twitter argued that denying standing to Harris placed an undue burden on Twitter, who was thereby forced to either comply with, or move to quash, each such subpoena seeking information of a Twitter user that it receives. The court flatly disagreed, noting that "that burden is placed on *every* third-party respondent to a subpoena and cannot be used to create standing for a defendant where none exists."

No Undue Burden Under the Stored Communications Act

A court issuing an order under Section 2703(d) of the SCA, "on a motion made promptly by the service provider," may quash or modify the order if it finds that the information or records sought are "unusually voluminous" or if compliance with the order "otherwise would cause an undue burden" on the service provider. In this case, the order requires Twitter to provide all user information associated with the @destructuremal Twitter account, including all tweets posted from it between September 15, 2011, and December 31, 2011. The court declined to find that this order placed an undue burden on Twitter under the SCA, stating instead that "it does not take much to search and provide the data to the court."



Sources: http://blog.flurry.com, http://blog.hubspot.com, http://tag.microsoft.com.

Warrant Required for Tweets in Electronic Storage for Less Than 180 Days

The only data associated with the @destructuremal account that the court did not order Twitter to produce were those tweets sent out from the account

on December 31, 2011. This is because, under the SCA, the court may compel either an Electronic Communications Service (ECS) or a Remote Computing Service (RCS) to disclose non-content information, and may compel an RCS to disclose its contents; but the court may only compel an ECS to disclose content that has been in electronic storage for more than 180 days. At the time that the June 30, 2012 order was issued, the court did not have the proper authority under the SCA to order disclosure of tweets made on December 31, 2011. The court, accordingly, modified its previous order with respect to the ECS content that was less than 180 days old—removing that portion of the order that would have required Twitter to produce tweets placed from the @destructuremal account on December 31, 2011.

What Next?

The Criminal Court of the City of New York ordered Twitter to disclose all non-content information, as well as all content information from September 15, 2011, to December 30, 2011. As noted, Twitter has announced its intention to appeal, rather than to comply with, the decision. Twitter will not have to turn over the December 31, 2011 tweets unless the government obtains a search warrant. Will Twitter have to turn over the other @destructuremal tweets? We'll keep you posted.

The NLRB Weighs In (Again) on Social Media Policies

With the issuance of its third guidance document on workplace social media policies in the past year, the National Labor Relations Board (NLRB) continues to refine its position on how to craft workplace social media policies that are consistent with the terms of the National Labor Relations Act (NLRA).

Section 7 of the NLRA provides employees with the right to engage in "concerted activities for the purpose of collective bargaining or other mutual aid or protection." This right applies regardless of whether the employees are members of a labor union. The NLRB's guidance on this subject suggests that employee social media policies that discourage the exercise of these rights may run afoul of the NLRA.

The NLRB's third memorandum, issued by Acting General Counsel Lafe Solomon, analyzes in detail seven different social media policies at issue in recent cases before the NLRB. Six of these policies were found by the NLRB to contain provisions that are contrary to the NLRA, while the seventh "revised" policy was upheld in its entirety as lawful. The NLRB specifically questioned the breadth of the following types of provisions, many of which are commonly found in social media policies:

- **Prohibitions on the disclosure of confidential or "non-public" information, or of matters concerning individual privacy rights, via social media.** Instructions not to reveal non-public information may be unenforceable as applied to discussions about, or criticism of, the employer's labor policies and its treatment of employees. The NLRB noted such a tension in policy requiring social media users not to "reveal non-public company information on any public site," where the explanation of non-public company information did not include appropriate carve-outs for activities protected under Section 7.

- **Prohibitions on the disclosure of an individual's personal information via social media.** The NLRB took issue with a social media policy instructing employees: "[D] on't disclose [personal information regarding employees and other third parties] in any way via social media or other online activities." As the NLRB explained, "[I]n the absence of clarification, employees would reasonably construe it to include information about employee wages and their working conditions."

- **Discouragements of the "friending" of one's co-workers.** According to the third memorandum, a policy statement advising employees to "think carefully about 'friending' other co-workers" could be construed as unlawfully discouraging employees from communicating regarding the terms of their employment.

- **Requirements that employee grievances be addressed through internal procedures, rather than aired online.** A social media policy providing the employer "believes that individuals are more likely to resolve concerns about work by speaking directly with co-workers, supervisors or other management-level personnel than by posting complaints on the Internet" was found to be unlawful, according to the NLRB, because it might inhibit employees from "seeking redress through alternative forums." The NLRB noted, however, that employers may "reasonably suggest" availing of internal dispute resolution procedures.

- **Prohibitions on the sending of unsolicited communications to other employees.** The NLRB found a policy requiring employees to report receiving "unsolicited or inappropriate electronic communications" to be an impermissible restraint on employees' right to discuss their employment conditions.

- **Restrictions on public discussions of personal opinions regarding work.** One policy discussed in the memorandum expressly permitted employees to discuss online their personal opinions about work-related issues, but only to other employees and not to the general public. The NLRB found this overbroad because the right to discuss employment conditions extends to discussions with non-employees.

- **Prohibitions on comments regarding pending legal matters.** A policy providing, "Don't comment on any legal matters, including pending

litigation or disputes," was found to be unlawful on the basis that it "restricts employees from discussing the protected subject of potential claims" against their employer.

- **Prohibitions on responding to government inquiries.** The NLRB found that one employer's direction to employees not to respond to communications from government agencies was overbroad "to the extent that it restricts employees from their protected right to converse with [NLRB] agents or otherwise concertedly seek the help of government agencies regarding working conditions, or respond to inquiries from government agencies regarding the same."
- **Requirements that employees check with the legal department or human resources (HR) department prior to posting or communicating with the media.** Requiring employees to secure permission from their employer before engaging in activities protected under Section 7, the memorandum noted, is prohibited by the NLRA.

Analyzing employer social media policies under the NLRA continues to be a major enforcement priority of the NLRB, although the NLRB's position on social media policies remains, for the most part, untested by the courts. The third memorandum underscores how the precise wording of the policy is critical to whether it is considered overbroad by the NLRB. Social media policies that distinguish between the prohibited behavior and concerted activities excluded by the policy, and that provide examples of each, would be more likely to withstand NLRB scrutiny. By contrast, the third memorandum cautions employers against relying on a so-called "savings clause" (such as a general statement that the policy will not be interpreted in a manner inconsistent with the NLRA) if "employees would not understand from this disclaimer that protected activities are in fact permitted."

Alongside its long list of examples of potentially unlawful policy language, the third memorandum provides one example of a social media policy that it considered lawful. Although this exemplar, which is attached to the NLRB memorandum in full, will not meet the needs of all employers, it may serve useful as a resource against which to compare your company's social media policy. As the NLRB's position on this subject evolves, we suggest consulting counsel to address whether specific provisions of your company's social media policy are consistent with the NLRB's guidance.

Look Before You Leap: Amazon Web Services Customers May Be Subject to an IP Covenant Not to Sue

The growth of cloud computing has been phenomenal, as companies ranging from early stage start-ups to conservative, blue-chip corporations have sought to take advantage of the cost savings offered by cloud-based solutions. And at the head of this revolution has been Amazon Web Services (AWS), one of the earliest and most popular of the cloud service providers. Indeed, AWS's cloud platform has proven to be particularly appealing to bloggers, website operators, social media providers and companies seeking to quickly and cost-effectively expand their presence on the Internet.

We have summarized elsewhere the privacy and data security concerns associated with cloud solutions, particularly those based on "public cloud" models. However, in recently reviewing the click-wrap "AWS Customer Agreement" governing access to and use of AWS, among the many standard pro-vendor provisions typically found in any online Terms of Use these days, we were struck by one provision that stood out as being highly unusual and particularly worrisome for AWS corporate users, especially users in the technology industry.

In Section 8.5 of the AWS Customer Agreement, AWS obtains from its customers a covenant not to sue for patent infringement or other intellectual property infringement in connection with AWS-related services. Here's the relevant language:

> "During and after the Term, you will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our affiliates, customers, vendors, business partners, or licensors, any patent infringement or other intellectual property infringement claim regarding any Service Offerings you have used."

Read literally, this language would appear to impose a covenant on AWS customers not to sue AWS—or its affiliates, customers, vendors, business partners or licensors—for patent, copyright or other intellectual property infringement in connection with web services made available not only by AWS but also by its affiliates. Immunized services purport to include not only AWS's data hosting services but also associated application programming interfaces and content (although content made available by third parties on the AWS platform would appear to be excluded).

Moreover, if enforceable, the covenant language would prohibit AWS customers from authorizing, assisting or encouraging any third party to pursue intellectual property-related claims against AWS, its affiliates, customers, vendors, business partners or licensors, a broad prohibition that could—if read in the broadest fashion—potentially impact law firms and other entities that provide assistance to patent, copyright and other intellectual property owners.

And the kicker? The provision purports to survive the expiration or termination of the AWS Customer Agreement. So a company's decision to terminate its

relationship with AWS may not relieve such company of its obligations under the "do not assert" provision.

For a number of legal reasons, companies should always proceed with caution whenever considering the use of a cloud platform. Conducting thorough due diligence is essential, and, of course, such due diligence requires careful review of all agreements or policies governing one's access to or use of the platform under consideration. And, as the AWS Customer Agreement illustrates, companies that have patents or other intellectual property rights covering Internet or cloud-related technologies or works need to be particularly vigilant that, in their drive to reduce storage costs, they are not inadvertently restricting their ability to fully exploit their intellectual property rights.

Face Off: Consumer Sues Hockey Team Over Text Messages

Earlier this year, Fred Weiss, a Pittsburgh Penguins hockey team fan, responded to an offer to receive text messages alerting him to team news and special offers. Although the terms pertaining to the call-to-action apparently promised Weiss that he would receive no more than three messages per week, he alleges that he received five messages the first week and four the following week. Instead of simply following the alerts' unsubscribe instructions, Weiss filed a putative class action lawsuit against the hockey team, alleging that its delivery of more messages than promised violated the federal Telephone Consumer Protection Act (TCPA).

The TCPA generally prohibits the delivery of a text message without the recipient's express consent. In his complaint, Weiss has alleged that the delivery of messages in excess of those to which he had agreed (i.e., three per week) was without his express consent, and, for each of those violating messages, he says that he—and his fellow class members—should therefore receive the prescribed statutory damages of at least $500. Statutory damages per violating message could go up to as much as $1,500 if the Penguins are found to have willfully or knowingly violated the law.

Companies sending text messages to consumers need to ensure that they are in compliance with their own representations regarding such messages.

Some may wonder why the Penguins would have made a message frequency promise in the first place. Widely followed industry guidelines issued by the Mobile Marketing Association (MMA) state that a marketer should provide certain information to consumers when seeking their consent to receive recurring text messages—including the fact that the consumer's mobile carrier's message and data rates apply, as well as how many messages the consumer can expect to receive. These disclosures give the consumer the information that he or she needs to make an informed decision regarding whether to sign up. The MMA guidelines do not have the force of law, but they are intended to help ensure that marketers comply with mobile carrier requirements. Moreover, while a message frequency disclosure is not expressly prescribed by law, the Federal Trade Commission (FTC) or a state regulator could take the position that a failure to tell a consumer, before he or she subscribes, how many messages to expect is an omission of material information and therefore deceptive. Marketers are therefore advised to make the disclosures imposed by the MMA guidelines.

As the ongoing Penguins litigation highlights, however, making the disclosures is not enough: the marketer must also take care to abide by its own promises. A failure to do so may give rise not only to a private cause of action under the TCPA—a very hot area for plaintiffs' attorneys over the past couple of years—but could also lead to an enforcement action by the FTC or a state regulator, charging that the marketer's failure to follow its own promises was deceptive. The bottom line is that companies sending text messages to consumers need to ensure that they are in compliance with their own representations regarding such messages, or they may find themselves in the penalty box.

The Social Media Experiment: Challenges for Broker-Dealers and Investment Advisers

The news that a Wall Street firm plans to give its financial advisers limited access to social media websites has been viewed by many as inevitable. Morgan Stanley's foray into the fast-changing world of social media highlights the difficulties faced by broker-dealers and investment advisers and the regulators who oversee them. As more financial firms follow suit, regulators will struggle to enforce securities laws that were written when the telephone and the telegraph were the prevailing social media.

Federal securities laws require broker-dealers and investment advisers to comply with a panoply of detailed rules designed to ensure that customers and clients are not misled. The rules require them to keep records of every paragraph, sentence, and word—and now, every tweet.

The challenge: how can financial firms comply with these strict rules while satisfying the market's growing passion for communicating by texts and tweets? And how can regulators enforce two-dimensional securities laws in the new three-dimensional world?

The exponential jump in social media usage has attracted the attention of federal securities regulators, who have responded with additional guidance and enforcement actions.

The exponential jump in social media usage has attracted the attention of federal securities regulators, who have responded with additional guidance and enforcement actions.

The Financial Industry Regulatory Authority (FINRA), which regulates broker-dealers, published guidance on blogs and social networking websites in January 2010. This was followed by guidance on social networking websites and business communications, posted in August 2011.

In January 2012, the U.S. Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) published a National Examination Risk Alert called Investment Adviser Use of Social Media, which outlines in stark terms the SEC staff's compliance concerns on the use of social media by registered investment advisers.

While investors typically do not distinguish between broker-dealers, on one hand, and registered investment advisers, on the other hand, these two types of financial institutions are regulated under similar, but very different, sets of rules. Social media use by investment advisers that are dually registered with the SEC and with FINRA is subject to both sets of rules and interpretations.

Investment advisers. The SEC has recognized that social media is "landscape-shifting" and that its use by the financial services industry is rapidly accelerating.

The SEC staff has stated its view that use of social media to communicate with clients and prospective clients may implicate Rule 206(4)-1 under the Investment Advisers Act of 1940, as amended (Advisers Act), which governs advertisements by investment advisers.

This rule, in relevant part, provides that an investment adviser will violate the Advisers Act's anti-fraud provisions if it publishes, circulates, or distributes "any advertisement" that:

- Refers, directly or indirectly, to "testimonials of any kind concerning the investment adviser" or the investment advice it provides;
- Refers, directly or indirectly, to past specific recommendations it provided (e.g., "cherry picking"), unless the adviser discloses a list of all recommendations, subject to certain requirements;
- Represents that a graph, chart, or formula, by itself, can be used to determine which securities to buy, without prescribed disclosures;
- Contains a statement to the effect that a report, analysis, or other service will be furnished free of charge, unless it is actually provided entirely free of charge without condition; or
- Contains any untrue statement of a material fact, or that is otherwise false or misleading.

The SEC defines "advertisement" very broadly. "Advertisements" include, in relevant part, any notice, circular, letter, or other written communication addressed to more than one person, or any notice or announcement in any publication or by radio or television, that (1) offers analysis, report, or publication concerning securities, or that is to be used in making any determination as to when to buy or sell any security, or (2) any graph, chart, formula, or other device to be used in making any determination as to when to buy or sell any security, or (3) any other investment advisory service with regard to securities.

While this regulatory definition reflects technological advancements through and including the cathode ray tube television set, we can reasonably conclude that it applies to all kinds of social media communications, including blogs, wikis, photo and video sharing, podcasts, social networking, and virtual worlds.

OCIE's regulatory concerns can be categorized into three broad categories: compliance policies and procedures, third-party content, and record keeping.

Compliance programs. First, the SEC staff is concerned that investment adviser compliance programs may include overlapping procedures that apply to advertisements and communications but do not specifically include social media. The staff urges investment advisers to evaluate the effectiveness of their compliance programs with respect to the use of social media by the firms themselves, their representatives, or solicitors, including the following hot buttons:

- *Usage guidelines.* Compliance procedures should address appropriate usage and restrictions on use of social media, based on potential risks.
- *Content standards.* Content may implicate fiduciary duties or other regulatory issues, which compliance procedures should address.

- *Monitoring.* Advisers should consider how to monitor use of social media by employees, representatives, and solicitors, and should take into consideration the lack of ability to monitor third-party sites.
- *Frequency of monitoring.* The staff suggests a risk-based approach for frequency of monitoring of social media communications.
- *Approval of content.* Advisers should consider pre-approval of communications, rather than after-the-fact reviews.
- *Firm resources.* Advisers should evaluate their resources to ensure that they are sufficient to adequately monitor personnel and archive communications.
- *Criteria for approving participation.* Compliance procedures should assess risks to the adviser, including operational, reputational, privacy, and other regulatory issues.
- *Training.* Advisers should consider implementing a training program related to social media, with a view toward promoting compliance.
- *Certification.* Consider procedures that require personnel to certify that they understand and will comply with social media policies.
- *Functionality.* Advisers should consider the functionality of social media sites approved for use, including the continuing obligation to address any upgrades or modifications.
- *Personal/professional sites.* Advisers should consider whether to adopt policies to address business conducted on personal or third-party media sites.
- *Information security.* Advisers should consider whether permitting representatives to have access to social media sites poses information security risks, and how to protect information.
- *Enterprise-wide sites.* Advisers that are part of a larger financial services or corporate enterprise may consider creation of usage guidelines designed to prevent the advertising practices of a firmwide social media site from violating the Advisers Act.

Third-party content. Second, the staff has indicated that third-party content on social media sites presents special compliance challenges. These issues arise when third parties post messages, forward links, or post articles to an adviser's website or in social media sites. Adviser representatives and solicitors generally do not interact with these third parties or respond to their postings.

The staff noted its concern about direct or indirect testimonials "of any kind." The SEC's rules do not define the term "testimonial," but the SEC's staff broadly interprets the term to include a statement of a client's experience with, or endorsement of, an investment adviser. Therefore, the use of "social plug-ins," *even when a third party hits the "Like" button on an adviser's Facebook page* could be a "testimonial" under the Advisers Act if the "Like" represents an explicit or implicit statement of a client's experience with an investment adviser or its representative.

The staff's concerns underscore the challenges that investment advisers face when the use of freewheeling, interactive social media collides with requirements to comply with pre-Internet regulations that were designed to regulate newspaper and magazine advertisements.

Recordkeeping. The SEC's third area of concern is recordkeeping obligations of advisers. OCIE noted that the recordkeeping rules do not differentiate between traditional paper communications, like snail mail, and electronic communications, such as emails, instant messages, and other ways that investment advisers provide advisory services. In other words, the federal regulators focus on the *content* of the communication, rather than its *form.* OCIE urges investment advisers to ensure that their recordkeeping policies and procedures allow advisers that use social media to comply with the recordkeeping requirements.

In January 2012, the SEC published an Investor Alert, Social Media and Investing: Avoiding Fraud, designed to make investors aware of fraudulent investment schemes that use social media. It also provides tips for checking the backgrounds of investment advisers and brokers. An Investor Bulletin, Social Media and Investing, Understanding Your Accounts provides tips for investors who use social media about privacy settings, security, and password selection.

Also in January 2012, the Enforcement Division announced that the SEC charged an Illinois-based investment adviser with offering to sell fictitious securities on LinkedIn. Among other things, the Division alleged that the adviser used LinkedIn discussions to promote fictitious "bank guarantees" and "medium term notes," which generated interest from potential investors. The adviser failed to comply with recordkeeping requirements or maintain a required Code of Ethics.

The SEC's Enforcement Division noted that fraudsters are quick to adapt to new technologies to exploit them for unlawful purposes. This case suggests that the federal regulators are determined to adapt to new technologies to follow the fraud.

Broker-dealers. As long ago as 1999, FINRA recognized the potential compliance issues posed by use of social media when it stated that a registered representative's participation in an Internet chat room is subject to the same requirements as a presentation in person before a group of investors. FINRA codified this guidance in 2003, when it defined the term "public appearance" to include participation in an interactive electronic forum.

FINRA published its Guide to the Internet for Registered Representatives, and in

September 2011, it released a three-part series of podcasts on these issues to educate broker-dealers and their representatives.

FINRA is not so much concerned about the form of a communication from a registered representative; rather, it is concerned about the content of the communication and whether the registered representative obtained prior supervisory approval for sending the communication. FINRA penalized a registered representative who posted 32 tweets touting a particular security without prior principal approval, among other alleged violations.

For a summary of recent FINRA concerns about social networking, see our August 3, 2011 News Bulletin, FINRA to Issue More Guidance on Social Media.

The Morgan Stanley initiative. The New York Times DealB%k reported on June 25, 2012 that, after a yearlong trial program, Morgan Stanley planned to give about 17,000 financial advisers "partial access" to Twitter and LinkedIn. But don't expect their registered representatives to get carried away with a flurry of on-the-fly stock picks. The representatives draw posts "from a prewritten library" of Twitter messages and submit all LinkedIn postings for approval, using advanced software designed for this purpose. Other firms likely will follow suit and devote more resources to developing this latest frontier of communications with customers.

Not only did Morgan Stanley give the green light to its financial advisers to post limited tweets, but, on the firm's official Twitter account, senior Morgan Stanley economists recently tweeted their analysis of the U.S. jobs report and the European Central Bank's decision to lower interest rates.

This initiative signals a trajectory and confirms that the financial services industry's use of social media is here to stay. And it is a somber reminder that, notwithstanding advances in communications technology, firms must still comply with pre-Internet federal securities laws covering anti-fraud, advertising, and recordkeeping.

We note that regulated entities also need to pay attention to the growing tension between guidance on social media use issued by regulators and new laws and National Labor Relations Board pronouncements imposing restrictions on employers' ability to monitor or curtail their employees' social media use.

An additional challenge. We note that regulated entities also should understand the growing tension between, on one hand, the typically conservative guidance on social media use issued by regulators and, on the other hand, new laws and National Labor Relations Board pronouncements restricting employers' ability to monitor or curtail their employees' social media use. There are no easy solutions to this emerging issue; rather, a company's chief compliance officer and its employment law advisors should coordinate polices in an effort to alleviate the tension between these conflicting regulatory approaches.

Conclusion. The exponential growth of the use of social media presents compliance and operational challenges for investment advisers and broker-dealers. Regulators are devoting more and more resources as they scramble to stay current with technological advances in this area. Financial services firms are well advised to assess how their customers and employees use social media, to evaluate the potential risks, and to ensure that their policies and procedures adequately address the increasingly complex compliance and operational issues arising from the soaring popularity of social media.

What, What (in the Court): South Park Studios Shielded by Fair Use for Viral Video Parody

The Seventh Circuit held recently in *Brownmark Films, LLC v. Comedy Partners* that, under certain circumstances, a trial court may dismiss a copyright infringement case based on a fair use defense prior to discovery.

Over the years, the satiric Comedy Central cartoon program *South Park* and its creators have developed a reputation for biting social commentary. Past targets include World of Warcraft players, Occupy Wall Street, and the History Channel's recent obsession with swamp creatures and World War II. In the show's 12th season, in an episode entitled "Canada on Strike," *South Park* took on the world of viral videos. The episode included a parody of a real-world viral video called "What What (In the Butt)" ("WWITB") (Authors' Note: possibly NSFW). *South Park's* version visually approximates the original, but plays on the naïveté of the starring nine-year-old *South Park* character, Butters, by using more childish elements; for example, by portraying Butters dressed up as a teddy bear and a daisy.

Brownmark, the copyright holder for the original WWITB video, filed suit for copyright infringement against South Park Digital Studios and others ("South Park Studios"). South Park Studios responded with a motion to dismiss based on an

affirmative fair use defense. Although Circuit Judge Cudahy noted that courts should generally refrain from dismissing cases based on affirmative defenses, he wrote that the reason for this reticence is that defenses typically turn on facts that emerge during discovery and trial. In this case, though, the district court ruled that only two pieces of evidence were needed to decide the question of fair use: the original WWITB video and South Park Studios' parody.

The district court granted South Park Studios' motion and dismissed the case. The Seventh Circuit affirmed, noting that "[o]ne only needs to take a fleeting glance at the South Park episode" to determine that its use of the WWITB video is meant "to lampoon the recent craze in our society of watching video clips on the internet . . . of rather low artistic sophistication and quality." Thus, fair use.

Other commentators support the decision, noting that the focus of the parody is not the specific viral video, but rather that the parody is a commentary on society's consumption of such Internet videos generally. It is worth noting that such arguments have not always found favor in the courts. For example, in the well-known *Cat Not in the Hat! case*, a district court found—and the Ninth Circuit affirmed—that a book entitled *The Cat Not in the Hat! A Parody by Dr. Juice* was not shielded as fair use. The book "mimic[ked] the distinctive style" of a Dr. Seuss book, using repetitive, simple rhymes to tell the story of the O.J. Simpson double-murder trial. The general idea is that a use is not fair if, in the words of the U.S. Supreme Court in *Campbell v. Acuff-Rose*, the alleged infringer uses the original work solely "to get attention or to avoid the drudgery in working up something fresh." In *Brownmark*, it seems, the Seventh Circuit viewed *South Park's* parody as something more than mere drudgery avoidance.

Going forward, *Brownmark* changes little, if anything, with respect to the substance of the fair use analysis. But *Brownmark* does show that courts may—in at least some fair use cases and at least in the Seventh Circuit—grant a motion to dismiss prior to discovery. While *Brownmark* involved a seemingly easy fair use case in the defendants' favor, it will be interesting to see whether future courts will grant motions to dismiss where the fair use analysis is less obvious. In any event, copyright infringement plaintiffs should be aware that the road to discovery where a defendant raises a fair use defense may not be quite as smooth as it used to be.

California Attorney General Creates Privacy Enforcement and Protection Unit; Increased Enforcement Likely

On July 19th, California Attorney General Kamala D. Harris announced the formation of a new Privacy Enforcement and Protection Unit within the state's Department of Justice. The move is widely seen as a means of stepping up the state's enforcement activities involving privacy issues.

The Privacy Enforcement and Protection Unit will be organized under the state's new eCrime Unit, which was formed in August 2011, and will centralize a number of existing California Justice Department programs intended to enforce privacy laws, combat identity theft, educate consumers, and create partnerships with private industry under one umbrella. The new unit's mission is broad: it will enforce federal and state laws regulating the collection, retention, disclosure, and destruction of private or sensitive information by individuals, organizations, and the government. In addition to traditional online privacy, the unit's mandate covers health privacy, financial privacy, identity theft, government records, and data breach laws. The unit will be staffed by California Department of Justice employees, including six dedicated prosecutors.

Harris has made online privacy protection a major focus of her administration, and the creation of the new Privacy Enforcement and Protection and eCrime Units are just two of her initiatives aimed at fighting online crime and protecting consumer privacy. In February of this year, Harris also secured an agreement between her office and the six major platforms for distributing and selling mobile applications. The agreement is designed to ensure that mobile and social apps comply with the California Online Privacy Protection Act, which requires operators of commercial websites and online services that collect personally identifiable information about Californians to conspicuously post a privacy policy. Facebook signed onto the agreement, called a "Joint Statement of Principles," in June 2012, adding the primary platform for social applications to the agreement.