SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

Volume 4, Issue 1 January/February 2013

IN THIS ISSUE

Employers and Employees Battle Over Social Media Accounts
Page 2

Anonymous P2P User's Motion to Quash Subpoena Denied
Page 3

FTC Snuffs Out Online "History Sniffing"
Page 4

Socially Aware Looks Back: The Social Media Law Year in Review
Page 5

AdWords Decision Highlights Contours of CDA Section 230 Safe Harbor
Page 7

FCC Rules That Opt-Out Confirmation Text Messages Do Not Violate TCPA
Page 8

Facebook 'em, Danno: Is the Hawaii 5-0's Facebook Wall A Public Forum?
Page 9

PeopleBrowsr Wins Round One Against Twitter
Page 10

EDITORS

John Delaney
Gabriel Meister
Aaron Rubin

CONTRIBUTORS

Amanda M.F. Bakale
Tiffany Cheung
Adam J. Fleisher
Matthew R. Galeotti
Jacob Michael Kaufman
J. Alexander Lawrence
Christine E. Lyon
Julie O'Neill
Jesse K. Soslow

In this issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media, we explore the challenges that arise when employers and employees battle over work-related social media accounts; we discuss a new litigation trend in which content owners are focusing on individual P2P users to enforce their rights, despite potential First Amendment hurdles; we report on the FTC's crackdown on so-called "history sniffing"; we examine how Section 230 of the Communications Decency Act may or may not fully protect website operators from trademark-related claims; we review a recent FCC ruling on whether opt-out confirmation text messages violate the Telephone Consumer Protection Act; we highlight constitutional challenges to how public entities moderate their social media pages; we summarize a recent order requiring Twitter to continue to provide PeopleBrowsr with access to Twitter's "Firehose"; and we recap major events from 2012 that have had a substantial impact on the law of social media.

All this, plus a collection of eye-opening numbers on the use of social media in 2012.

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

MORRISON FOERSTER

EMPLOYERS AND EMPLOYEES BATTLE OVER SOCIAL MEDIA ACCOUNTS

When an employee uses a social media account to promote his or her company, who keeps that account when the employee leaves? Perhaps more importantly, who keeps the friends, followers and connections associated with that account? Three lawsuits highlight the challenges an employer may face in seeking to gain control of work-related social media accounts maintained by current or former employees.

We start with *Eagle v. Edcomm*, a federal case out of Pennsylvania involving a dispute over an ex-employee's LinkedIn account and related connections. The plaintiff, Dr. Linda Eagle, was a co-founder of the defendant company, Edcomm. She established a LinkedIn account while at Edcomm, using the account to promote the company and to build her network. Edcomm personnel had access to her LinkedIn password and helped to maintain the account. Following termination of her employment, Edcomm allegedly changed Dr. Eagle's LinkedIn password and her account profile; the new profile displayed the new interim CEO's name and photograph instead of Dr. Eagle's. (Apparently, "individuals searching for Dr. Eagle were routed to a LinkedIn page featuring [the new CEO]'s name and photograph, but Dr. Eagle's honors and awards, recommendations, and connections.") Both parties raced to the courthouse, filing lawsuits against each other over the LinkedIn account and other disputes. Although a final ruling on all of the issues has not yet been made, the court has issued two decisions.

In the earlier of the two decisions, the court granted Dr. Eagle's motion to dismiss Edcomm's trade secret misappropriation claim, concluding that the LinkedIn connections were not a trade secret because they are "either generally known in the wider business community or capable of being easily derived from public information."

The most recent decision, however, was largely a win for Edcomm. The court granted Edcomm's motion for summary judgment on Dr. Eagle's Computer Fraud and Abuse Act (CFAA) and Lanham Act claims. Regarding her CFAA claims, the court concluded that the damages Dr. Eagle claimed she had suffered—related to harm to reputation, goodwill and business opportunities—were insufficient to satisfy the "loss" element of a CFAA claim, which requires some relation to "the impairment or damage to a computer or computer system." In rejecting Dr. Eagle's claim that Edcomm violated the Lanham Act by posting the new CEO's name and picture on Dr. Eagle's LinkedIn account, the court found that Dr. Eagle could not demonstrate that Edcomm's actions caused a "likelihood of confusion," as required by the Act.

Three recent cases illustrate the importance of creating clear policies on the treatment of business-related social media accounts, and making sure employees are aware of these policies.

In a federal case out of Illinois, *Maremont v. Susan Fredman Design Group LTD*, the employee, Jill Maremont, was seriously injured in a car accident and had to spend several months rehabilitating away from work. While recovering, Ms. Maremont's employer—Susan Fredman Design Group—posted and tweeted promotional messages on Ms. Maremont's private Facebook and Twitter accounts, where she had developed a large following as a well-known interior designer. The posts and tweets continued after Ms. Maremont had asked her employer to stop, so Ms. Maremont changed her passwords. Following the password changes, Ms. Maremont alleged that her employer started treating her poorly in order to force her to resign. Ms. Maremont then brought claims under the Lanham Act, Illinois' Right of Publicity Act, and the common law right to privacy. Although the case is still pending, the court issued a decision refusing to dismiss Ms. Maremont's Lanham Act and Right of Publicity Act claims. The court, however, dismissed her common law right to privacy claims, holding that she had failed to demonstrate that her employer's "intrusion into her personal 'digital life' is actionable under the common law theory of unreasonable intrusion upon the seclusion of another," and that she had failed to allege a false light claim because she did not allege that her employer "acted with actual malice."

A recently-settled California case, *PhoneDog LLC v. Noah Kravitz*, about which we have written previously, involved a similar dispute over a former employee's Twitter account. Unlike the LinkedIn account at issue in the *Edcomm* case, the Twitter account in *PhoneDog* apparently was created by the employer, not the employee—however, the Twitter "handle" identifying the account included both the employer's name and the employee's name: @PhoneDog_Noah. According to PhoneDog's complaint, the account attracted approximately 17,000 Twitter followers. Mr. Kravitz, who after leaving PhoneDog eventually began working for one of PhoneDog's competitors, kept the Twitter account but removed PhoneDog's name, changing the account's handle to @noahkravitz. PhoneDog sued Mr. Kravitz, alleging that Mr. Kravitz wrongfully used the Twitter account to compete unfairly against PhoneDog. Like Edcomm, PhoneDog alleged misappropriation of trade secrets, although PhoneDog appears to have viewed the account log-in information rather than the actual followers as the relevant trade secret information.

As noted above, the parties have settled the *PhoneDog* case, so we will not learn how the court would have ultimately ruled; nevertheless, this case and the other pending suits discussed above offer important lessons to employers. Although the terms of the settlement are confidential, news reports have indicated that the agreement does allow Mr. Kravitz to keep his Twitter account and followers.

These cases have received media attention, and the two pending cases—*Eagle* and *Maremont*—will continue to be closely watched by the legal community to see how courts define ownership interests in employee social media accounts. Employers, however, should not wait on the rulings in these pending cases to take steps to protect their interests in their social media accounts. All three of these cases illustrate the importance of creating clear policies regarding the treatment of business-related social media accounts, and making sure that employees are aware of these policies. Other measures an employer can take include being certain to control the passwords of the company's own social media accounts, and making sure that the name of the account does not include an individual employee's name. At the same time, employers need to be mindful of new laws in California restricting an employer's ability to gain access to its employees' personal social media accounts, laws on which we have reported previously. And of course, in light of these developments, it remains particularly important to maintain a clear distinction between company and personal social media accounts.

ANONYMOUS P2P USER'S MOTION TO QUASH SUBPOENA DENIED

BitTorrent, the peer-to-peer (P2P) file-sharing system that enables the quick downloading of large files, has sparked another novel controversy stemming from copyright-infringement claims brought against its users. Users take advantage of the BitTorrent sharing system to anonymously access popular media such as books and movies. That anonymity is unlikely to last long for users who are alleged to have downloaded copyrighted material. Last month, Judge Sweet, a federal judge in the Southern District of New York (SDNY), held that an anonymous P2P user has no First Amendment right to quash a subpoena seeking her identity where the plaintiff had no other means to effectively identify the defendant.

Wiley reflects a new wave of litigation in which copyright holders have shifted from suing host sites to focusing on individual users of P2P networks.

In *John Wiley & Sons Inc. v. Does Nos. 1-35*, the plaintiff (Wiley), a publisher of books and journal articles, alleged that unidentified "John Does" used BitTorrent to illegally copy and distribute Wiley's copyrighted works and infringe on Wiley's trademarks. Wiley sued 35 defendants known only by their "John Doe Numbers" and Internet Protocol (IP) addresses. Seeking to identify the Does, Wiley moved for court-issued subpoenas to be served on various Internet service providers (ISPs), ordering them to supply identifying information corresponding to the Does' IP addresses. In an attempt to maintain her anonymity and avoid liability, one of the 35 Does, then known only as John Doe No. 25 ("Doe 25") or IP Address 74.68.143.193, moved to quash a subpoena served on her ISP, Time Warner Cable.

Wiley reflects a new wave of litigation in which copyright holders have shifted from suing host sites to focusing on individual users of P2P networks. The mere fact that copyrighted material is downloaded from a particular IP address may be insufficient to prove that the P2P network user is the infringer. An IP address typically provides only the location at which one of any number of devices may be used by any number of individuals (in fact, Doe 25 contended that her ex-husband, not she, downloaded the infringing works). If a motion to quash is granted, the account holder's identity is not revealed, and the claim is effectively dead.

In considering whether to grant an anonymous account holder's motion to quash a subpoena, courts balance the user's First Amendment right to act anonymously with the plaintiff's right to pursue its claims.

Anonymous users can rely on a line of precedent that extends the First Amendment's protections to online expression. And under Rule 45 of the Federal Rules of Civil Procedure, a court must quash a subpoena if it requires disclosure of protected matter. Thus, to the extent that anonymity is protected by the First Amendment, courts will quash subpoenas designed to breach anonymity.

On the other hand, plaintiffs pursuing their claims can point to precedent holding that the First Amendment may not be used to encroach upon the intellectual property rights of others.

To balance these competing principles and determine whether certain actions trigger First Amendment protection, courts weigh the five factors set out in *Sony Music Entertainment Inc. v. Does 1-40*:

- whether the plaintiff has made a concrete showing of actionable harm;
- the specificity of the discovery request;
- the absence of alternative means by which to obtain the subpoenaed information;
- a central need for the data; and
- the party's expectation of privacy.

In *Wiley*, each of these five factors weighed in favor of disclosure of the defendant's identity. Wiley pled a sufficiently specific claim of copyright infringement, and, without a subpoena, Wiley would have

no other effective way to identify potential infringers of Wiley's intellectual property rights.

At least five other courts within the SDNY have denied motions to quash in similar litigations involving defendants accused of infringing Wiley's copyrights via BitTorrent. Going forward, so long as copyright holders can satisfy the *Sony* five-factor test, they will be able to rely on cases like *Wiley* to ferret out copyright infringers.

FTC SNUFFS OUT ONLINE "HISTORY SNIFFING"

The Federal Trade Commission (FTC) has cracked down on a company that was engaged in "history sniffing," a means of online tracking that digs up information displayed by web browsers to reveal the websites that users have visited. In a proposed settlement with Epic Marketplace, Inc. and Epic Media Group (together, "EMG") that was announced on December 5, 2012, the FTC settled charges that EMG had improperly used history sniffing to collect sensitive information regarding unsuspecting consumers.

EMG functions as an intermediary between publishers—i.e., websites that publish advertisements—and the advertisers who want to place their ads on those websites. It performs this function through online behavioral advertising, which typically entails placing cookies on websites that a consumer visits in order to collect information about his or her use of the website, and then using that information to serve targeted ads to the user when he or she visits other websites within the "EMG Marketplace Network," the network of publisher websites serviced by EMG.

What got EMG into trouble was that EMG also used history sniffing to collect information regarding what websites users had visited. Here's how the technique works at a high level: In your web browser, hyperlinks to websites change color once you've visited them. For example, if you

Continued on page 7

BIGGEST NUMBERS IN SOCIAL MEDIA FROM 2012

810,000 – the number of retweets of President Obama's 2012 election victory tweet—the most retweeted post on Twitter *ever* [1]

4 million – the number of Facebook "likes" for President Obama's 2012 election victory post—the most liked Facebook photo *of all time* [2]

200 million – the number of LinkedIn members as of January 9, 2013 [3]

1 billion – the number of views of PSY's **"Gangnam Style"**—the most viewed YouTube video in history [4]

1 billion – the number of monthly active Facebook users as of October 2012 [5]

1.1 billion – the number of photos uploaded to Facebook over New Year's Eve and New Year's Day [6]

3 billion – the total number of Foursquare "check-ins" from its inception through 2012 [7]

4 billion – the number of hours of video watched on YouTube every month [8]

1. https://twitter.com/BarackObama/status/266031293945503744/photo/1
2. http://news.cnet.com/8301-17938_105-57546254-1/obama-victory-photo-smashes-facebook-like-record/
3. http://blog.linkedin.com/2013/01/09/linkedin-200-million/
4. http://news.cnet.com/8301-1023_3-57560498-93/gangnam-style-the-first-video-to-hit-1b-youtube-views/
5. http://finance.yahoo.com/news/number-active-users-facebook-over-230449748.html
6. http://techcrunch.com/2013/01/17/facebook-photos-record/
7. http://thenextweb.com/location/2012/11/21/foursquare-has-its-3-billionth-check-in-seeing-growth-of-x/
8. http://www.youtube.com/t/press_statistics

SOCIALLY AWARE LOOKS BACK: THE SOCIAL MEDIA LAW YEAR IN REVIEW

2012 was a momentous year for social media law. We've combed through the court decisions, the legislative initiatives, the regulatory actions and the corporate trends to identify what we believe to be the ten most significant social media law developments of the past year–here they are, in no particular order:

Bland v. Roberts – A Facebook "like" is not constitutionally protected speech

Former employees of the Hamptons Sheriff's Office in Virginia who were fired by Sheriff BJ Roberts, sued claiming they were fired for having supported an opposing candidate in a local election. Two of the plaintiffs had "liked" the opposing candidate's Facebook page, which they claimed was an act of constitutionally protected speech. A federal district court in Virginia, however, ruled that a Facebook "like" ". . . is insufficient speech to merit constitutional protection"; according to the court, "liking" involves no actual statement, and constitutionally protected speech could not be inferred from "one click of a button."

This case explored the increasingly-important intersection of free speech and social media with the court finding that a "like" was insufficient to warrant constitutional protection. The decision has provoked much criticism, and it will be interesting to see whether other courts will follow the *Bland* court's lead or take a different approach.

New York v. Harris – Twitter required to turn over user's information and tweets

In early 2012, the New York City District Attorney's Office subpoenaed Twitter to produce information and tweets related to the account of Malcolm Harris, an Occupy Wall Street protester who was arrested while protesting on the Brooklyn Bridge. Harris first sought to quash the subpoena, but the court denied the motion, finding that Harris had no proprietary interest in the tweets and therefore did not have standing to quash the subpoena. Twitter then filed a motion to quash, but the court also denied its motion, finding that Harris had no reasonable expectation of privacy in his tweets, and that, for the majority of the information sought, no search warrant was required.

This case set an important precedent for production of information related to social media accounts in criminal suits. Under the *Harris* court's ruling, in certain circumstances, a criminal defendant has no ability to challenge a subpoena that seeks certain social media account information and posts.

The National Labor Relations Board (NLRB) issued its third guidance document on workplace social media policies

The NLRB issued guidance regarding its interpretation of the National Labor Relations Act (NLRA) and its application to employer social media policies. In its guidance document, the NLRB stated that certain types of provisions should not be included in social media policies, including: prohibitions on disclosure of confidential information where there are no carve-outs for discussion of an employer's labor policies and its treatment of employees; prohibitions on disclosures of an individual's personal information via social media where such prohibitions could be construed as limiting an employee's ability to discuss wages and working conditions; discouragements of "friending" and sending unsolicited messages to one's co-workers; and prohibitions on comments regarding pending legal matters to the degree such prohibitions might restrict employees from discussing potential claims against their employer.

The NLRB's third guidance document illustrates the growing importance of social media policies in the workplace. With social media becoming an ever-increasing means of expression, employers must take care to craft social media policies that do not hinder their employees' rights. If your company has not updated its social media policy in the past year, it is likely to be outdated.

Fteja v. Facebook, Inc. and *Twitter, Inc. v. Skootle Corp.* – Courts ruled that the forum selection clauses in Facebook's and Twitter's terms of service are enforceable

In the *Fteja* case, a New York federal court held that a forum selection clause contained in Facebook's Statement of Rights and Responsibilities (its "Terms") was enforceable. Facebook sought to transfer a suit filed against it from a New York federal court to one in Northern California, citing the forum selection clause in the Terms. The court found that the plaintiff's clicking of the "I accept" button when registering for Facebook constituted his assent to the Terms even though he may not have actually reviewed the Terms, which were made available via hyperlink during registration.

In the *Skootle* case, Twitter brought suit in the Northern District of California against various defendants for their spamming activities on Twitter's service. One defendant, Garland Harris, who was a resident of Florida, brought a motion to dismiss, claiming lack of personal jurisdiction and improper venue. The court denied Harris's motion, finding that the forum selection clause in Twitter's terms of service applied. The court, however, specifically noted that it was not finding that forum selection clauses in "clickwrap" agreements are generally enforceable, but rather "only that on the allegations in this case, it is not unreasonable to enforce the clause here."

Fteja and *Skootle* highlight that potentially burdensome provisions in online agreements may be enforceable even as to consumers; in both cases, a consumer seeking to pursue or defend a claim against a social media platform provider was required to do so in the provider's forum. Both consumers and businesses need to be mindful of what they are agreeing to when signing up for online services.

Six states passed legislation regarding employers' access to employee/applicant social media accounts

California, Delaware, Illinois, Maryland, Michigan and New Jersey enacted legislation that prohibits an employer from requesting or requiring an employee or applicant to disclose a user name or password for his or her personal social media account.

Such legislation will likely become more prevalent in 2013; Texas has a similar proposed bill, and California has proposed a bill that would expand its current protections for private employees to also include public employees.

Facebook goes public

Facebook raised over $16 billion in its initial public offering, which was one of the most highly anticipated IPOs in recent history and the largest tech IPO in U.S. history. Facebook's peak share price during the first day of trading hit $45 per share, but with a rocky first few months fell to approximately $18—sparking shareholder lawsuits. By the end of 2012, however, Facebook had rebounded to over $26 per share.

Facebook's IPO was not only a big event for Facebook and its investors, but also for other social media services and technology startups generally. Many viewed, and continue to view, Facebook's success or failure as a bellwether for the viability of social media and technology startup valuations.

Employer-employee litigation over ownership of social media accounts

2012 saw the settlement of one case, and continued litigation in two other cases, all involving the ownership of business-related social media accounts maintained by current or former employees.

In the settled case of *PhoneDog LLC v. Noah Kravitz*, employer sued employee after the employee left the company but retained a Twitter account (and its 17,000 followers) that he had maintained while working for the employer. The terms of the settlement are confidential, but news reports indicated that the settlement allowed the employee to keep the account and its followers.

In two other pending cases, *Eagle v. Edcomm* and *Maremont v. Susan Fredman Design Group LTD*, social media accounts originally created by employees were later altered or used by the employer without the employees' consent.

These cases are reminders that, with the growing prevalence of business-related social media, employers need to create clear policies regarding the treatment of work-related social media accounts.

California's Attorney General went after companies whose mobile apps allegedly did not have adequate privacy policies

Starting in late October 2012, California's Attorney General gave notice to developers of approximately 100 mobile apps that they were in violation of California's Online Privacy Protection Act (OPPA), a law that, among other things, requires developers of mobile apps that collect personally identifiable information to "conspicuously post" a privacy policy. Then, in December 2012, California's Attorney General filed its first suit under OPPA against Delta, for failing to have a privacy policy that specifically mentioned one of its mobile apps and for failing to have a privacy policy that was sufficiently accessible to consumers of that app.

Privacy policies for mobile applications continue to become more important as the use of apps becomes more widespread. California's OPPA has led the charge, but other states and the federal government may follow. In September, for instance, Representative Ed Markey of Massachusetts introduced The Mobile Device Privacy Act in the U.S. House of Representatives, which in some ways would have similar notice requirements as California's OPPA.

Changes to Instagram's online terms of service and privacy policy created user backlash

In mid-December 2012, Instagram released an updated version of its online terms of service and privacy policy (collectively, "Terms"). The updated Terms would have allowed Instagram to use a user's likeness and photographs in advertisements without compensation. There was a strong backlash from users over the updated Terms, which ultimately led to Instagram apologizing to its users for the advertisement-related changes, and reverting to its previous language regarding advertisements.

Instagram's changes to its Terms, and subsequent reversal, are reminders of how monetizing social media services is often a difficult balancing act. Although social media services need to figure out how they can be profitable, they also need to pay attention to their users' concerns.

The defeat of the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA)

Two bills, SOPA and PIPA—which were introduced in the U.S. House of Representatives and U.S. Senate, respectively, in late 2011—would have given additional tools to the U.S. Attorney General and intellectual property rights holders to combat online intellectual property infringement. A strong outcry, however, arose against the bills from various Internet, technology and social media companies. The opponents of the bills, who claimed the proposed legislation threatened free speech and innovation, engaged in various protests that included "blacking out" websites for a day. These protests ultimately resulted in the defeat of these bills in January 2012.

The opposition to and subsequent defeat of SOPA and PIPA demonstrated the power of Internet and social media services to shape the national debate and sway lawmakers. With prominent social media services such as Facebook, YouTube, Twitter, LinkedIn and Tumblr opposed to the bills, significant public and, ultimately, congressional opposition followed. Now that we've witnessed the power that these services wield when acting in unison, it will be interesting to see what issues unite them in the future.

Continued from page 4

have never visited a particular website with your browser, hyperlinks to that site will typically appear in your browser in one color (e.g., blue), whereas once you've visited the website, hyperlinks to the site will appear in a different color (e.g., purple). History sniffing code exploits this feature by "sniffing" around a web page displayed in your browser to see what color your hyperlinks are. When the code finds purple links, it knows that you've already visited those websites—and thereby, the code catches a glimpse of your browsing history.

According to the FTC, for almost 18 months—from March 2010 until August 2011—EMG included history sniffing code in ads that it served to website visitors on at least 24,000 web pages within its network, including web pages associated with name brand websites. EMG used such code to determine whether consumers had visited more than 54,000 different domains, including websites "relating to fertility issues, impotence, menopause, incontinence, disability insurance, credit repair, debt relief, and personal bankruptcy." EMG used this sensitive information to sort consumers into "interest segments" that, in turn, included sensitive categories like "Incontinence," "Arthritis," "Memory Improvement," and "Pregnancy-Fertility Getting Pregnant." EMG then used these sensitive interest segments to deliver targeted ads to consumers.

History sniffing is not per se illegal under U.S. law. What got EMG into trouble was that it allegedly misrepresented how it tracked consumers. First, EMG's privacy policy at the time stated that the company only collected information about visits to websites *within the EMG network*; however, the FTC alleged that the history sniffing code enabled EMG to "determine whether consumers had visited webpages that were outside the [EMG] Marketplace Network, information it would not otherwise have been able to obtain." EMG's tracking of users in a manner inconsistent with its privacy policy was therefore allegedly deceptive, in violation of Section 5 of the FTC Act.

Second, EMG's privacy policy did not disclose that the company was engaged in history sniffing; it disclosed only that it "receives and records anonymous information that your browser sends whenever you visit a website which is part of the [EMG] Marketplace Network." According to the FTC, the fact that the company engaged in history sniffing would have been material to consumers in deciding whether to use EMG's opt-out mechanism. EMG's failure to disclose the practice was therefore also allegedly deceptive in violation of Section 5 of the FTC Act.

If you collect data in a manner inconsistent with—or not disclosed in—your privacy policy, you run the risk of a charge of deception in violation of Section 5 of the FTC Act.

The proposed consent order would, among other things, require EMG to destroy all of the information that it collected using history sniffing; bar it from collecting any data through history sniffing; prohibit it from using or disclosing any information that was collected through history sniffing; and bar misrepresentations regarding how the company collects and uses data from consumers or about its use of history sniffing code.

EMG ceased its history sniffing in August 2011, and most new versions of web browsers have technology that blocks this practice. Nonetheless, the FTC made it clear in its complaint that it wanted to highlight the problem because history sniffing "circumvents the most common and widely known method consumers use to prevent online tracking: deleting cookies." Mark Eichorn, assistant director of the FTC's Division of Privacy and Identity Protection, told the *Los Angeles Times* that the FTC "really wanted to make a statement with this case." He added, "People, I think, really didn't know that this was going on and didn't have any reason to know." The proposed consent order puts online tracking and advertising companies on notice: If you collect data in a manner inconsistent with—or not disclosed in—your privacy policy, you run the risk of a charge of deception.

ADWORDS DECISION HIGHLIGHTS CONTOURS OF CDA SECTION 230 SAFE HARBOR

In a string of cases against Google, approximately 20 separate plaintiffs have claimed that, through advertisements on its AdWords service, Google engaged in trademark infringement. These claims have been based on Google allowing its advertisers to use their competitors' trademarks in Google-generated online advertisements. In a recent decision emerging from these cases, *CYBERsitter v. Google*, the U.S. District Court for the Central District of California found that Section 230 of the Communications Decency Act (CDA) provides protection for Google against some of the plaintiff's state law claims.

As we have discussed previously (including in both 2012 and 2011), Section 230 states that "[n]o 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." The Section 230 safe harbor immunizes websites from liability for content created by users, as long as the website

did not "materially contribute" to the development or creation of the content. An important limitation on this safe harbor, however, is that it shall not "be construed to limit or expand any law pertaining to intellectual property."

In the *CYBERsitter* case, plaintiff CYBERsitter, which sells an Internet content-filtering program, sued Google for selling and displaying advertisements incorporating the CYBERsitter trademark to ContentWatch, one of CYBERsitter's competitors. CYBERsitter's complaint alleged that Google had violated numerous federal and California laws by, first, selling the right to use CYBERsitter's trademark to ContentWatch and, second, permitting and encouraging ContentWatch to use the CYBERsitter mark in Google's AdWords advertising. Specifically, CYBERsitter's complaint included claims of trademark infringement, contributory trademark infringement, false advertising, unfair competition and unjust enrichment.

Google filed a motion to dismiss, arguing that Section 230 of the CDA shielded it from liability for CYBERsitter's state law claims. The court agreed with Google for the state law claims of trademark infringement, contributory trademark infringement, unfair competition and unjust enrichment, but only to the extent that those claims sought to hold Google liable for the infringing content of the advertisements. The court, however, did not discuss the apparent inapplicability of the Section 230 safe harbor to trademark claims. As noted above, Section 230 does not apply to intellectual property claims and, despite the fact that trademarks are a form of intellectual property, the court applied Section 230 without further note. This is because the Ninth Circuit has held that the term "intellectual property" in Section 230 of the CDA refers to *federal* intellectual property law and therefore *state* intellectual property law claims are *not* excluded from the safe harbor. The Ninth Circuit, however, appears to be an outlier with this interpretation; decisions from other circuit courts suggest disagreement with the Ninth Circuit's approach, and district courts outside the Ninth Circuit have not followed the Ninth Circuit's lead.

The Ninth Circuit refused to let Google off entirely with regard to CYBERsitter's state trademark law claims—distinguishing between Google's liability for the content of AdWords advertisements, and its liability for potentially tortious conduct unrelated to the content of such advertisements.

Google was not let off the hook entirely with regard to the plaintiff's state trademark law claims. In dismissing the trademark infringement and contributory trademark infringement claims, the court distinguished between Google's liability for the content of the advertisements and its liability for its potentially tortious conduct unrelated to the content of the advertisements. The court refused to dismiss these claims to the extent they sought to hold Google liable for selling to third parties the right to use CYBERsitter's trademark, and for encouraging and facilitating third parties to use CYBERsitter's trademark, without CYBERsitter's authorization. Because such action by Google has nothing to do with the online content of the advertisements, the court held that Section 230 is inapplicable.

The court also found that CYBERsitter's false advertising claim was not barred by Section 230 because Google may have "materially contributed" to the content of the advertisements and, therefore, under Section 230 would have been an "information content provider" and not immune from liability. Prof. Eric Goldman, who blogs frequently on CDA-related matters, has pointed out an apparent inconsistency in the *CYBERsitter* court's reasoning, noting that Google did not materially contribute to the content of the advertisements for the purposes of the trademark infringement, contributory infringement, unfair competition and unjust enrichment claims, but that Google might have done so for the purposes of the false advertising claim.

CYBERsitter highlights at least two key points for website operators, bloggers, and other providers of interactive computer services. First, at least in the Ninth Circuit, but not necessarily in other circuits, the Section 230 safe harbor provides protection from state intellectual property law claims with regard to user-generated content. Second, to be protected under the Section 230 safe harbor, the service provider must not have created the content *and* it must not have materially contributed to such content's creation.

FCC RULES THAT OPT-OUT CONFIRMATION TEXT MESSAGES DO NOT VIOLATE TCPA

As noted in our *Socially Aware* blog last September, waves of class actions have recently alleged that the delivery of an opt-out confirmation text message violates the Telephone Consumer Protection Act (TCPA). Thus, a Federal Communications Commission ("Commission") Declaratory Ruling finding that a single opt-out confirmation text does not violate the TCPA comes at a crucial time. The Commission's decision, issued on November 29, 2012, is a welcome relief to companies facing these cases.

The TCPA generally permits the delivery of text messages to consumers after receiving prior express consent to do so. Numerous plaintiffs have taken the position that an opt-out confirmation message violates the TCPA because it is delivered after consent has been revoked. In its ruling, however, the Commission found that a consumer's prior express consent to receive a text message can be reasonably construed to include consent to receive a final, one-time message confirming that the consumer has revoked such consent. Specifically, delivery of an opt-out confirmation text message does not violate the TCPA provided that it (1) merely confirms the consumer's opt-out request and does not include any marketing or promotional information, *and* (2) is the only message sent to the consumer after receipt of his or her opt-out request. In addition, the Commission explained that if the opt-out confirmation text is sent within five minutes of receipt of the opt-out, it will be presumed to fall within the consumer's prior express consent. If it takes longer, however, "the sender will have to make a showing that such delay was reasonable and the longer this delay, the more difficult it will be to demonstrate that such messages fall within the original prior consent."

The Commission's ruling brings the TCPA into harmony with widely followed self-regulatory guidelines issued by the Mobile Marketing Association, which affirmatively recommend that a confirmation text be sent to the subscriber after receiving an opt-out request. The ruling also comes on the heels of, and is consistent with, at least two recent decisions in putative class action cases filed in the Southern District of California. In *Ryabyshchuck v. Citibank (South Dakota) N.A.*, the court held that Citibank did not violate the TCPA by sending a text message confirming that it had received the customer's opt-out request. The court went as far as to say that "common sense renders the [opt-out] text inactionable under the TCPA." The court reasoned that the TCPA was intended to shield consumers from the proliferation of intrusive, nuisance communications,

A recent FCC ruling clarifies whether opt-out confirmation text messages delivered after consent has been revoked violate the Telephone Consumer Protection Act.

and "[s]uch simple, confirmatory responses to plaintiff-initiated contact can hardly be termed an invasion of privacy under the TCPA." Likewise, in *Ibey v. Taco Bell Corp.*, the court dismissed a lawsuit alleging that Taco Bell had violated the TCPA by sending an opt-out confirmation message. Noting that the TCPA was enacted to prevent unsolicited and mass communications, the court held, "[to] impose liability ... for a single, confirmatory text message would contravene public policy and the spirit of the statute—prevention of unsolicited telemarketing in a bulk format."

The Commission's ruling should bring an end to the rash of class actions brought in recent months challenging the legality of confirmatory opt-out messages.

FACEBOOK 'EM, DANNO: IS THE HAWAII 5-0'S FACEBOOK WALL A PUBLIC FORUM?

On top of a presidential election, protests over Instagram's terms of use, and the invention of gloves that can translate sign language, 2012 also brought to light interesting constitutional issues involving public entities' use of social media, when a citizens' group filed suit against the City and County of Honolulu for "violations of [the group's] freedoms of speech" based on the Honolulu Police Department's removal of several of the group's postings from the Department's official Facebook page.

The background of the lawsuit is seemingly innocuous. Like the White House, the City of New York, and other governmental entities, the Honolulu Police Department ("HPD") has an official Facebook page. The HPD uses its Facebook page to provide the citizens of Honolulu with everything from crime reports to information on public parking, and Facebook users are able to comment on its various posts. For a period of time, HPD also allowed Facebook members to post on its "wall." (HPD no longer allows wall posts, but retains a "recommendations box" on its page where users can make comments.) Starting in the beginning of 2012, several members of the Hawaii Defense Foundation (the "Foundation"), a non-profit organization dedicated to training citizens to use handguns and informing Hawaiians of their rights regarding firearms, began posting comments, articles, and photographs on the HPD Facebook page's wall, criticizing the HPD on issues ranging from restrictions on issuing concealed weapons permits to alleged corruption. The administrators of the HPD Facebook page took the same actions that administrators of other Facebook pages commonly take: deleting the offensive posts and blocking the posters, both of which are easily accomplished using Facebook's interface.

Although individuals and private companies take these actions every day on their Facebook pages, the Foundation pointed out that the HPD Facebook page was a self-proclaimed "forum open to the public" created and administered by a government entity. Facebook describes the HPD and other such bodies as "Government Organizations," although this label is applied merely for categorization purposes and does not purport to carry any legal weight. Nonetheless, the Foundation labeled the administrators of the page as "agents" of the city of Honolulu, and

Complaints against administrators of Facebook pages that serve as "public forums" raise new policy issues that did not exist in the pre-social media era.

argued that their actions were subject to scrutiny under the First and Fourteenth Amendments. In its complaint, the Foundation cited *Rosenberger v. Rector and Visitors of the University of Virginia*, a case in which a university's fund for student activities was considered a "limited public forum" for First Amendment purposes, to demonstrate that "a forum *need not* be a physical place." The Foundation also claimed that the HPD violated its Fourteenth Amendment rights by removing the posts and banning the group's members in violation of the Foundation members' due process rights.

Although the Foundation's suit against the HPD is the first First Amendment suit of its kind, depending on its outcome, other private groups may soon file similar complaints against "Government Organizations" on Facebook that take a similarly aggressive approach to administering their Facebook pages. In fact, a former police officer in the small village of Island Lake, Illinois recently requested review from the Illinois Attorney General's office when his comments on Island Lake's Facebook page were deleted by the page's administrators. The Illinois Attorney General issued an opinion in which it found that Island Lake's actions did not violate the Illinois Open Meetings Act, but the opinion did not address the First Amendment issues.

The Foundation's suit against the HPD and other complaints against administrators of Facebook pages that serve as "public forums" raise policy issues that did not exist in the pre-social media era. Unlike more conventional forms of criticizing the government, such as holding up physical signs in front of city, state or federal buildings, Facebook can be used as a vehicle for dissent from the privacy of one's own home and enables the complaining individual to make his or her opinions instantly known to the entire Internet-equipped world. Although governmental entities are not required to have Facebook pages, they often establish such pages as a simple and efficient way of conveying information to citizens. If these entities are to face constant constitutional scrutiny based on their means of administering their Facebook pages, they may be reluctant to maintain social media presences. The White House Facebook page endures an endless onslaught of criticism in the form of comments on its posts (although it does not allow users to post on its wall); on the other hand, the Island Lake Facebook page appears to have been shut down for the most part. In light of the HPD and Island Lake complaints, one legal commentator advises public schools whose Facebook pages may be visited by disgruntled students to "consult with legal counsel before deleting comments from social media webpages to address the constitutionality of that action."

Regardless of the HPD suit's outcome, the fact that the complaint was filed in the first place reinforces the notion that social media is the new battleground for all aspects of the law, from intellectual property to criminal law... and now, the frontier of constitutionality.

PEOPLEBROWSR WINS ROUND ONE AGAINST TWITTER

The Superior Court of the State of California has entered a temporary restraining order requiring Twitter to continue to provide PeopleBrowsr with access to the Firehose, Twitter's complete stream of all public tweets. Through the Firehose, Twitter provides third-party access to over 400 million daily tweets.

PeopleBrowsr is a San Francisco-based social media analytics firm that provides custom applications to clients ranging from private businesses, consumers and publishers to government agencies. PeopleBrowsr's data mining and analytics platforms support various products and services, such as data streams, social media command centers and consumer targeting programs. For example, PeopleBrowsr's product Kred provides a real-time measure of social influence within social media user networks.

Through its Firehose, Twitter provides third-party access to over *400 million* daily tweets.

PeopleBrowsr's business depends on its continued access to user-generated social media content from Twitter. Twitter's recent decision to restrict PeopleBrowsr's access to the Firehose led PeopleBrowsr to sue Twitter in California state court in order to protect its current business model.

PeopleBrowsr and Twitter had entered into a license agreement in June 2010, enabling PeopleBrowsr to receive access to the Firehose in exchange for over $1 million a year. Twitter recently invoked a contractual provision that allowed Twitter to terminate the agreement without cause. PeopleBrowsr filed a complaint for interference with contractual relations, in which it claimed that its products and services require access to the Twitter Firehose in order to provide clients with contextual data analysis. In response, Twitter claimed that it had decided not to renew most of its direct-to-user Firehose contracts, instead reselling Twitter data in various forms through intermediaries. Without

full access to the Firehose, PeopleBrowsr claimed, it could not provide the products that its customers expected. According to PeopleBrowsr, it needs access to the Firehose in order to detect and analyze emerging trends fully and quickly; all tweets in the Firehose are necessary to conduct the scoring and ranking of individual influence that underpins PeopleBrowsr's analysis.

On Twitter's motion, the case has been removed to federal court. PeopleBrowsr has filed a motion to remand back to state court, and Twitter has filed a motion to dismiss. Both motions remain pending before the Northern District of California.

As this case moves forward it promises to provide an in-depth look at the Twitter ecosystem and guidance for companies with business models that depend on access to data from social media companies such as Twitter. Stay tuned for further developments.

SOCIAL MEDIA 2013: ADDRESSING CORPORATE RISKS

Social media sites are transforming not only the daily lives of consumers, but also how companies interact with consumers. However, along with the exciting new marketing opportunities presented by social media come challenging new legal issues. In seeking to capitalize on the social media gold rush, is your company taking the time to identify and address the attendant legal risks?

Please join *Socially Aware* editor John Delaney as he chairs Practising Law Institute's (PLI) "Social Media 2013: Addressing Corporate Risks." Issues to be addressed at the conference include the following:

- **Social media: How it works, and why it is transforming the business world**
- **Drafting and updating social media policies**
- **User-generated content and related IP concerns**
- **Ensuring protection under the CDA's Safe Harbor**
- **Minimizing risks relating to mobile apps**
- **Online marketing: New opportunities, new risks**
- **Privacy law considerations**
- **Practical tips for handling real-world issues**

Representatives from Twitter, Google, Tumblr and other companies will be speaking at the event. The conference is being held in San Francisco on February 6, 2013 and in New York City on February 27, 2013; the February 6th event will be webcasted. For more information or to register, please visit PLI's website at www.pli.edu/content.