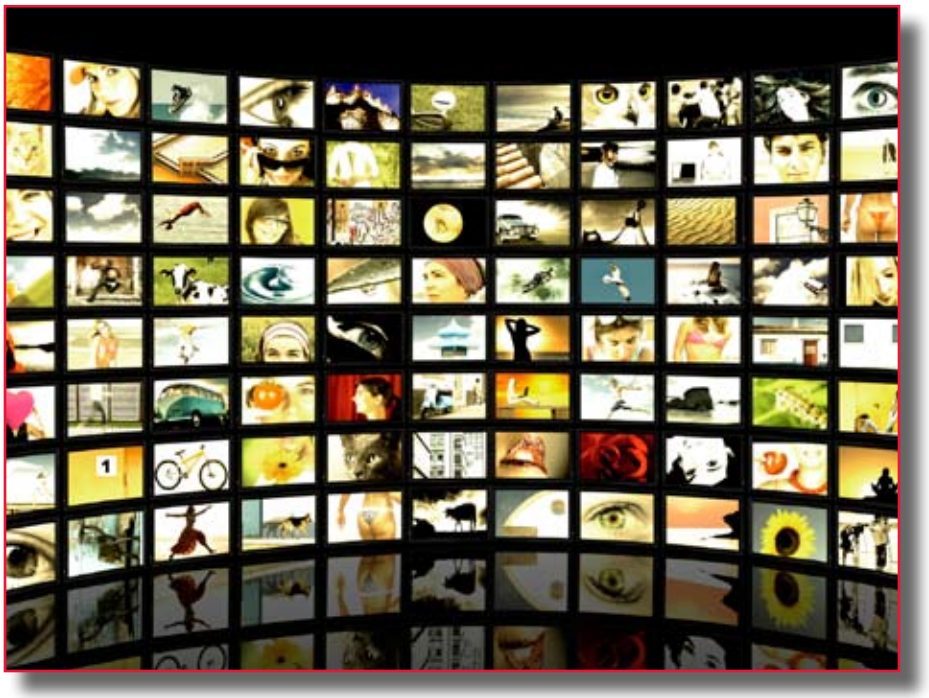
Morrison & Foerster Social Media Newsletter

Vol. 1, Issue 5 November 2010

Socially Aware:
The Social Media Law Update



In this issue of *Socially Aware*, our guide to the law and business of social media, we discuss how Google has revised the contractual terms governing use of its application programming interfaces to strike a blow at Facebook and, potentially, other online companies that rely on Google users' lists of contacts. We review two recent New York court decisions regarding the discovery of information posted to social media sites. We also provide an update on Facebook's ever-expanding portfolio of social media patents, and take a look at the latest firestorm over Facebook's privacy practices. We explore a recent New York City Bar Association opinion regarding ethical restrictions on "friending" social media users in order to gain access to evidence on their social media pages, and we highlight recently released government documents suggesting that federal agents may be monitoring U.S. citizenship applicants' social media activities for evidence of fraud. Finally, we provide a statistical snapshot of the most popular brands on Twitter.

IN THIS ISSUE

EDITORS

John Delaney
Gabriel Meister

CONTRIBUTORS

Kara Alesi
Maddy Batliboi
Emily Huters
Matt King
Aaron Rubin

Do Unto Others: Google API Terms Now Require Data Reciprocity

Google recently revised the terms applicable to its Contacts Data API and Portable Contacts API—i.e., the application programming interfaces that allow websites to import Google users' lists of contacts automatically—to require reciprocity. In other words, any website that uses Google's APIs to import Google users' contacts must provide similar data portability to its own users.

The relevant addition to Google's API Terms of Service is as follows: "Google supports data portability. By accessing Content through the Contacts Data API or Portable Contacts API for use in your service or application, you are agreeing to enable your users to export their contacts data to other services or applications of their choice in a way that's substantially as fast and easy as exporting such data from Google Contacts, subject to applicable laws."

Commentators have interpreted this change as Google's latest salvo in its war with Facebook. Previously, a Facebook user could easily import his or her Google contacts into Facebook, a functionality that Facebook provided to its users using Google's APIs. Facebook, however, has reportedly never permitted its own users to export their Facebook contact information, whether to other websites or to a standalone file. According to a statement from a Google spokesperson, sites that do not allow data portability, such as Facebook, "leave users in a data dead end." Therefore, argues Google, while Google users will still be free to export their contacts from Google, Google "will no longer allow websites to automate the import of users' Google Contacts (via [the Google] API) unless they allow similar export to other sites."

TOP 10 MOST POPULAR BRANDS ON TWITTER*

BRAND	FOLLOWERS
CNN	3,610,554
NY TIMES	2,730,044
GOOGLE	2,574,164
E! ONLINE	2,487,605
THE ONION	2,461,130
PEOPLE MAGAZINE	2,231,297
TIME MAGAZINE	2,232,663
NBA	2,149,768
MASHABLE	2,117,505
WHOLE FOODS	1,833,500

* As of November 15, 2010
Source: http://twittercounter.com

This means that, unless and until Facebook provides such reciprocity, Facebook users will not be able to import their Google contacts into Facebook automatically using Google's API (although Google users still are able to export their Google contacts into various file formats using Google Contacts' native export feature, and import contacts from those files into Facebook). Moreover, while the change in Google's API terms may have been directed primarily at Facebook, per the revised terms, any other service that uses the Google APIs must also comply with the revised terms and allow users to export their service's contacts "in a way that's substantially as fast and easy as exporting such data from Google Contacts."

Of course, it remains to be seen whether and to what extent Google may seek to enforce the reciprocity requirement against anyone other than Facebook, nevertheless, website operators that use the Google APIs should keep in mind the ancient Kenyan proverb, "When elephants fight, it is the grass that suffers."

Checking In: Facebook's Expanding Social Media Patent Portfolio

Following recent news that Facebook acquired 18 patents and patent applications formerly owned by Friendster, Facebook was recently awarded a patent addressing geolocation services. The patent, entitled "*Systems and methods for automatically locating web-based social network members*," includes claims such as, "a method of sharing locations of users participating in a social networking service at a geographic location," and purports to cover both manual updates of status information and updates through GPS-type systems—bringing to mind "check-ins," a popular social media functionality allowing friends to update one another on their current locations.

Caroline McCarthy at The Social notes that Facebook was not an early adopter of geolocation, and, indeed, only recently—in August 2010—launched

its own geolocation offering, Facebook Places. ITProPortal comments that, although Facebook joined the field later than Foursquare and other competitors, Facebook's 2007 patent filing shows that it may have started work on a geolocation feature earlier than expected. According to some commentators, as with Facebook's acquisition of the Friendster patents, the grant of the geolocation service patent could raise concerns for social media companies seeking to capitalize on the popularity of geolocation functionality.

Fake Friends: May a Lawyer Use Trickery to Access Information on Social Networking Sites?

Imagine that you are handling a divorce case and you learn that photographs providing evidence of the other spouse's infidelity are available on a Facebook page. Or perhaps you believe that certain YouTube videos set to "private" would provide evidence of infringement in your client's copyright case. You would like to obtain this helpful evidence, but you cannot access it unless you are "friends" with the Facebook or YouTube user who posted the material. May you send (or have your investigator send) a "friend request" to the user in order to gain access to evidence on the applicable social networking site?

According to a recent formal opinion from the New York City Bar Association's Committee on Professional Ethics (Formal Opinion 2010-2), the answer is no, if in doing so you engage in "trickery" or "deceptive behavior." The opinion includes examples of such prohibited behavior, such as creating a false Facebook profile listing schools, hobbies, interests, or other information likely to interest a targeted individual, and then using that profile to make a friend request "falsely portraying the attorney or investigator as the witness's long lost classmate, prospective employer, or friend of a friend." This type of conduct, the Committee concludes, violates the New York Rules of Professional Conduct, in particular Rule 4.1 ("[i]n the course of representing a client, a lawyer shall not knowingly make a false statement of law or fact to a third person") and Rule 8.4(c) ("[a] lawyer or law firm shall not… engage in conduct involving dishonesty, fraud, deceit, or misrepresentation").

The Committee also notes, however, that lawyers are not utterly prohibited from using social networking sites to contact potential witnesses and gather evidence. According to the opinion, such a blanket prohibition would be inconsistent with "the Court of Appeals' oft-cited policy in favor of informal discovery." Therefore, the Committee concludes, "an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request." The lesson for attorneys who wish to use social networking sites to contact witnesses and gather evidence, it seems, is "keep it real."

MAY YOU SEND (OR HAVE YOUR INVESTIGATOR SEND) A "FRIEND REQUEST" TO A SOCIAL MEDIA USER IN ORDER TO GAIN ACCESS TO EVIDENCE ON HIS OR HER SOCIAL MEDIA PAGE?

Facebook Apps Privacy Breach?

Privacy headaches have plagued Facebook all year. The company's privacy practices are again generating headlines; this time around, the focus is on allegations that Facebook applications transmit Facebook user IDs (i.e., unique numbers assigned to Facebook users by Facebook) to third party advertisers. The Wall Street Journal—found that "all of the 10 most popular apps on Facebook were transmitting users' IDs to outside companies." The Journal noted that "anyone can use an ID number to look up a person's name, using a standard Web browser, even if that person has set all of his or her Facebook information to be private," while "[f]or other users, the Facebook ID reveals information they have set to share with 'everyone,' including age, residence, occupation and photos."

According to a Facebook blog post, "in most cases, developers did not intend to pass this information, but did so because of the technical details of how browsers work." The Facebook blog post also claims that the press has exaggerated the implications of sharing a Facebook user ID because knowledge of the user ID "does not enable anyone to access private user information without explicit user consent."

Commentators have split over the seriousness of the alleged breach. Several commentators have voiced support for Facebook, with one observer noting that magazines, credit card companies and grocery store loyalty cards routinely disclose more information regarding customers than Facebook apps reveal.

Others have expressed alarm over the unauthorized transmission of Facebook user IDs. One commentator has warned that "allowing advertisers and other third parties to easily and definitively correlate a real name with an otherwise 'anonymous' IP address, cookie, or profile is a dangerous path forward for privacy." And as a Boing Boing blogger observed, "[T]his means you may have been compromised *even if you yourself didn't use the apps, but your friends did*."

Facebook has stated that the company would introduce new technology to address these concern.

New York Courts Continue to Define the Limits of Discovery of Information on Social Media Sites

A recent decision by a New York appellate court adds to the developing landscape of discovery of information on social media sites. Less than two months after a trial court in New York ordered a plaintiff to grant defendants access to her Facebook and MySpace pages, as discussed in the previous issue of Socially Aware, the court in *McCann v. Harleysville Insurance Company of New York* denied a similar request by a defendant to access the plaintiff's Facebook account. In both cases, the plaintiffs brought personal injury claims, and defendants sought discovery of information on the plaintiffs' social media sites as potentially relevant to the plaintiffs' alleged injuries.

At first glance, the *McCann* decision seems to be in conflict with the earlier case, *Romano v. Steelcase Inc.*, but a closer look reveals that the rulings may not actually be so far apart. In *Romano*, the defendant seeking discovery of information on the plaintiff's Facebook and MySpace pages put forth a strong argument for the relevancy of this information, noting that information on the publicly viewable portions of these pages showed the plaintiff engaging in various activities that contradicted her claims concerning the extent of her injuries. The *Romano* court cited to New York's broad discovery rules and the "strong public policy in favor of open disclosure" in finding it "reasonable to infer" from the postings on the plaintiff's public profile pages that "her private pages may contain materials and information that are relevant to her claims or that may lead to the disclosure of admissible evidence." The court thus ordered the plaintiff to grant defendants access to her Facebook and MySpace accounts.

Although the *McCann* defendant's arguments raised in support of its request for authorization to access the plaintiff's Facebook account are unclear from the published decision, the court found that the defendant "failed to establish a factual predicate with respect to the relevancy of the evidence" it sought. The court further found that the "defendant essentially sought permission to conduct 'a fishing expedition' into plaintiff's Facebook account based on the mere hope of finding relevant evidence." Importantly, however, the court left open the possibility for the defendant to bring a properly supported request for this information in the future. Indeed, as noted on the blog Internet Cases, if the defendant in McCann were to tailor its request more narrowly and make a clearer showing of the relevancy of the information requested, it might achieve the same success as the defendants in *Romano*.

I Spy: U.S. Government Monitoring of Social Media Sites

The federal government recently released documents indicating that it encourages federal agents to monitor U.S. citizenship applicants' social networking activity for proof of fraud. A memorandum by the U.S. Citizen and Immigration Services (USCIS) states: "*Narcissistic tendencies in many people fuels a need to have a large group of 'friends' link to their pages and many of these people accept cyber-friends that they don't even know. This provides an excellent vantage point for the [Office of Fraud Detection and National Security (FDNS)] to observe the daily life of beneficiaries and petitioners who are suspected of fraudulent activities*."

The memorandum suggests that tracking applicants' presence on social media sites such as Facebook, MySpace and Classmates.com, among other sites, could provide "an excellent vantage point" to observe the daily activities of those suspected of fraudulent activities.

The memorandum was released in response to an FOIA lawsuit on social network surveillance, filed in 2008 by the Electronic Frontier Foundation (EFF) in conjunction with the University of California Berkley's Samuleson Law, Technology, & Public Policy Clinic. In a recent press release, the EFF expressed concern that the USCIS failed to set forth a level of suspicion necessary before an agent could begin monitoring an applicant's social network presence, potentially making all applicants open to surveillance. Further, the EFF pointed out that the government's stance assumes that a person's online presence accurately portrays his or her offline life and "suggests there's nothing to prevent an exaggerated, harmless or even out-of-date off-hand comment in a status update from quickly becoming the subject of a full citizenship investigation." (Both the EFF and commentators note that social media profiles may not be the most accurate records of their users' lives, and may well contain false or misleading information, whether intentionally or unintentionally.) According to AOL News, however, USCIS spokesman Chris Bentley has stated that the USCIS "does not permit agency personnel to attempt to 'friend' immigration petitioners and their beneficiaries on social networks in an effort to reveal fraud."

If you wish to subscribe to *Socially Aware* or review earlier issues of *Socially Aware*, please click here or go to http://www.mofo.com/sociallyaware/.