Volume 6, Issue 4, October 2015

SOCIALLY AWARE

THE SOCIAL MEDIA LAW UPDATE

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

IN THIS ISSUE

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

Duane L. Carver, Jr.
Melissa M. Crespo
John F. Delaney
G. Larry Engel
Kristin A. Hiensch
J. Alexander Lawrence
Christine E. Lyon
Jake Joseph Perkowski
Anthony M. Ramirez
Aaron P. Rubin
Scott M. Sawyer

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

Welcome to the newest issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media. In this edition, we highlight five key social media law issues to address with your corporate clients; we discuss when social media posts are discoverable in litigation; we identify six important considerations in drafting legal terms for mobile apps; we take a look at the clash between bankruptcy law and privacy law in RadioShack's Chapter 11 proceedings; we examine a recent federal district court decision finding "browsewrap" terms of use to be of benefit to a website operator even if not a binding contract; we outline best practices for employers' use of social media to screen and interact with employees and conduct workplace investigations; we explore a Washington state court's refusal to unmask an anonymous online reviewer; and we discuss Facebook's recent update of its "Notes" feature.

All this—plus an infographic illustrating the growing popularity of video on social media.

FIVE SOCIAL MEDIA LAW ISSUES TO DISCUSS WITH YOUR CLIENTS

By Aaron P. Rubin and Scott M. Sawyer

The explosive growth of social media has clients facing legal questions that didn't even exist a few short years ago. Helping your clients navigate this muddled legal landscape will have them clicking "like" in no time.

WHAT'S IN A LIKE?

Not long ago, the word "like" was primarily a verb (and an interjection used by "valley girls"). You could have likes and dislikes in the sense of preferences, but you couldn't give someone a like, claim to own a like or assert legal rights in likes. Today, however, a company's social media pages and profiles, and the associated likes, followers and connections, are often considered valuable business assets. Courts have come to various conclusions regarding whether likes and similar social media constructs constitute property, but one thing is clear: Every company that uses social media should have in place clear policies regarding employee social media use and ownership of business-related social media accounts.

Employees who manage a company's social media accounts often insert themselves as the "voice" of the brand and establish a rapport with the company's fans and followers. Without clear policies that address ownership of social media accounts, and clearly distinguish between the company's accounts and employees' personal accounts, your client may find itself in a dispute when these employees leave the company and try to take the company's fans and followers with them.

Read a more detailed description of "likes" as assets here.

DIRTY LAUNDRY

It comes as no surprise that employees frequently use social media to complain about managers and coworkers, pay, work conditions and other aspects of their employment. Companies often would prefer not to air these issues publicly, so they establish policies and impose discipline when employees' social media activity becomes problematic. Companies need to be careful, however, that their policies and disciplinary actions comply with applicable law.

Without clear policies that address ownership of social media accounts, your client may find itself in a dispute when these employees leave the company and try to take the company's fans and followers with them.

A number of National Labor Relations Board decisions have examined whether employees' statements on social media constitute "concerted activity"—activity by two or more employees that provides mutual aid or protection regarding terms or conditions of employment—for purposes of the National Labor Relations Act (which, notably, applies regardless of whether the employees are unionized or not). Companies also need to be careful to comply with state statutes limiting employer access to employees' personal social media accounts, such as California Labor Code Section 980, which prohibits an employer from asking an employee or applicant to disclose personal social media usernames or passwords, access personal social media in the presence of the employer or divulge personal social media.

Read more about the intersection of social media policies and labor law here and here.

TERMS OF (AB)USE

Companies often consider their social media pages and profiles to be even more important than are the companies' own websites for marketing and maintaining customer engagement. But a company's own website has one advantage over a third-party social media platform: The company sets its own terms for use of its website, while the third-party social media platform is subject to terms of use imposed by the platform operator. And, in many cases, the terms imposed on users of social media platforms are onerous and make little distinction between individual users using the platform just for recreation and corporate users who depend on the platform for their businesses.

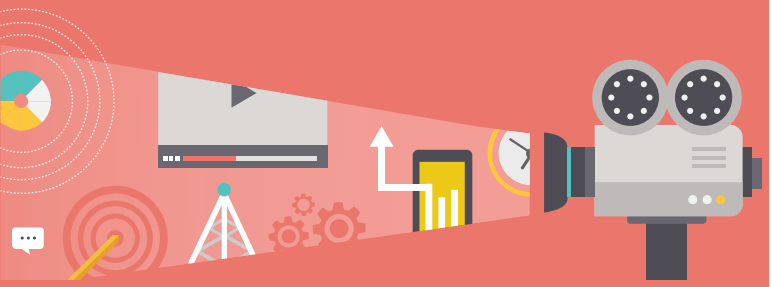
Social media terms of use often grant platform operators broad licenses to content posted on the platform, impose one-sided indemnification obligations on users and permit platform operators to terminate users' access with or without cause. You may have little luck negotiating modifications to such online contracts for your clients, but you can at least inform your clients of the terms that govern their use of social media so that they can weigh the costs and benefits.

Read more about social media platforms' terms of use here, here and here.

SAME AS IT EVER WAS

When it comes to using social media for advertising, the media may be new, but the rules are the same as ever. Companies that advertise through social media—especially by leveraging user endorsements—need to comply with Section 5 of the FTC Act, which bars "unfair or deceptive acts or practices." Bloggers and others who endorse products must actually use the product and must disclose any

VIDEO ON SOCIAL MEDIA



Last year, **94.1 million** U.S. users watched video on their mobile phones, up from 76.7 million in 2013.[1]

Online video will account for **69%** of consumer Internet traffic by 2017.[2]

A brand's unpaid post of a video to Facebook is **135% more likely** to be seen by its fans than its unpaid post of a photo:

A BRAND'S UNPAID DISTRIBUTION OF A VIDEO HAS AN **8.7%** CHANCE OF REACHING FANS.

THAT'S COMPARED TO AN UNPAID POST OF A PHOTO ON FACEBOOK, WHICH ONLY HAS A **3.7%** CHANCE OF REACHING FANS.[3]

U.S. desktop views of videos in August 2014:

ON GOOGLE SITES (INCLUDING YOUTUBE) **11.3 BILLION**

ON FACEBOOK **12.3 BILLION**[4]

IN DECEMBER 2014, BRANDS POSTED **20,000 MORE VIDEOS** ON FACEBOOK THAN ON YOUTUBE.*[5]

2 billion—THAT'S THE NUMBER OF VIDEOS WATCHED ON SNAPCHAT EVERY DAY.[6]

SOURCES

1 http://www.statista.com/statistics/209348/mobile-video-viewers-in-the-united-states/
2 http://www.theguardian.com/small-business-network/2014/jan/14/video-content-marketing-media-online
3 http://www.socialbakers.com/blog/2367-native-facebook-videos-get-more-reach-than-any-other-type-of-post
4 http://www.beet.tv/wp-content/uploads/2014/10/Slide09.jpg
5 http://www.business2community.com/video-marketing/3-notes-video-marketing-social-media-2015-01122766
6 http://www.businessinsider.com/snapchat-reaches-2-billion-video-views-daily-2015-5

*This is in large part due to Facebook's auto-play feature, which ensures that videos created on Facebook—and only videos created on Facebook—automatically play as users scroll down their newsfeeds.

"material connections" they have with the product providers (for example, a tech blogger reviewing a mobile phone that she received for free from the manufacturer should disclose that fact). Because this information is likely to affect consumers' assessment of an endorsement, failure to disclose may be deemed deceptive. So if you have a client that uses endorsements to promote its products, make sure to brush up on the FTC "Dot Com Disclosures" and other relevant FTC guidance.

Read more about endorsement disclosure obligations here.

GOOD REP

As noted, a company's social media pages, followers, etc., may constitute valuable business assets. But buyers in M&A transactions often neglect such assets when formulating the seller's reps and warranties. Buyers should consider asking the seller to disclose all social media accounts that the target company uses and to represent and warrant that none of the target's social media account names infringe any third-party trademark or other IP rights, that all use of the accounts complies with applicable terms of service and that the target has implemented policies providing that the company (and not any employee) owns all business-related social media accounts and imposing appropriate guidelines regarding employee use of social media.

Finally, if you have clients that use social media, it's important to be familiar with the popular social media platforms and their (ever-changing) rules and features. Learning to spot these issues isn't going to turn you into the next Shakira—as of this writing, the most liked person on Facebook with well over 100 million likes—but your clients will surely appreciate your help as they traverse the social media maze.

Read more about social media assets in M&A transactions here.

*(This piece originally appeared in **The Recorder**.)*

SOCIAL MEDIA E-DISCOVERY: ARE YOUR FACEBOOK POSTS DISCOVERABLE IN CIVIL LITIGATION?

By Jake Perkowski and J. Alexander Lawrence

Judge Richard J. Walsh began his opinion in *Largent v. Reed* with the following question: "What if the people in your life want to use your Facebook posts against you in a civil lawsuit?" With the explosive growth of social media, judges have had to confront this question more and more frequently. The answer to this question is something you'll hear quite often from lawyers: "It depends."

Courts generally have held that there can be no reasonable expectation of privacy in your profile when Facebook's homepage informs you that "Facebook helps you connect and share with the people in your life." Even when you decide to limit who can see your photos or read your status updates, that information still may be discoverable if you've posted a picture or updated a status that is relevant to a lawsuit in which you're involved. The issue, then, is whether the party seeking access to your social media profile has a legitimate basis for doing so.

If you've updated your Facebook status to brag about your awesome new workout routine after claiming serious and permanent physical injuries sustained in a car accident—yes, that information is relevant to a lawsuit arising from that accident and will be discoverable. The plaintiff in *Largent v. Reed* learned that lesson the hard way when she did just that, and the court ordered her to turn over her Facebook log-in information to the defense counsel. On the other hand, your Facebook profile will not be discoverable simply because your adversary decides he or she wants to go on a fishing expedition through the last eight years of your digital life.

Courts in many jurisdictions have applied the same standard to decide whether a litigant's Facebook posts will be discoverable: The party seeking your posts must show that the requested information may reasonably lead to the discovery of admissible evidence.

For example, the plaintiff in *Zimmerman v. Weis Markets, Inc.* claimed that he suffered permanent injuries sustained from operating a fork lift—and then went on to post that his interests included "ridin" and "bike stunts" on the public portion of his Facebook page. The court determined that his public posts placed the legitimacy of his damages claims in controversy and that his privacy interests did not outweigh the discovery requests.

In contrast, in *Tompkins v. Detroit Metropolitan Airport*, the plaintiff in this slip-and-fall case claimed back injuries in connection with an accident at the Detroit Metropolitan Airport. The defendant checked the plaintiff's publicly available Facebook photos (i.e., photos not subject to any of Facebook's available privacy settings or restrictions) and stumbled upon photos of the plaintiff holding a small dog and also pushing a shopping cart. The court determined that these photos were in no way inconsistent with the plaintiff's injury claims, stating that if "the Plaintiff's public Facebook page contained pictures of her playing golf or riding horseback, Defendant might have a stronger argument for delving into the nonpublic section of her account."

Facebook's privacy settings can provide at least some protection against discovery requests—assuming that the user has taken efforts not to display photos publicly that blatantly contradict his or her legal claims.

The *Tompkins* court recognized that the plaintiff's information was not discoverable because parties do not "have a generalized right to rummage at will through information" a person has posted. Indeed, the defendants sought the production of the plaintiff's *entire* Facebook account. Their overbroad and overreaching discovery request was—and is—common among parties seeking access to their opponents' Facebook data.

In response to these overbroad requests, courts routinely deny motions to compel the production of a person's entire Facebook profile because such requests are nothing more than fishing expeditions seeking what *might* be relevant information. As the court in *Potts v. Dollar Tree Stores, Inc.* stated, the defendant seeking Facebook data must at least "make a threshold showing that publicly available information on [Facebook] undermines the Plaintiff's claims."

The *Tompkins* and *Potts* decisions mark important developments in Facebook e-discovery cases. They establish that a person's entire Facebook profile is not discoverable merely because a portion of that profile is public. In turn, Facebook's privacy settings can provide at least some protection against discovery requests—assuming that the user has taken efforts not to display photos publicly that blatantly contradict his or her legal claims.

When it is shown that a party's Facebook history should be discoverable, however, the party must make sure not to tamper with that history. Deactivating your Facebook account to hide evidence can invite the ire of the court. Deleting your account outright can even result in sanctions. The takeaway is that courts treat social media data no differently than any other type of electronically stored information; what you share with friends online may also be something you share with your adversary—and even the court.

MOBILE APP LEGAL TERMS & CONDITIONS: SIX KEY CONSIDERATIONS

By John F. Delaney and Anthony M. Ramirez

For corporations, the mobile app is today's website.

Back in the late 1990s, no self-respecting company, no matter how

stodgy and old-fashioned, wanted to be without a website.

Today, the same is true with mobile apps. It doesn't matter what industry a company is in—it needs to have an app that customers and potential customers can download to their smartphones. Even big, tradition-bound law firms are developing and distributing mobile apps, for crying out loud.

Here at *Socially Aware*, we have been known to spend our free time downloading and examining mobile apps owned by companies that are new to the software distribution business (after all, a mobile app is just that—distributed software). In doing so, we've noticed a number of common missteps by app distributors in connection with the legal terms—or End User License Agreements (EULAs)—governing such apps. Accordingly, here is our list of key issues to address in adopting an EULA for a mobile app.

A EULA is an important part of any company's strategy to mitigate risks and protect its intellectual property in connection with its mobile apps.

1. Adopt Your Own EULA.

An EULA is an important part of any company's strategy to mitigate risks and protect its intellectual property in connection with its mobile apps. Hardly any company would release desktop software without an EULA, and mobile apps—which, as noted above, are software products—warrant the same protection. While Apple, Google and Amazon each provide a "default" EULA to govern mobile apps downloaded from their respective app stores, they also permit developers to adopt their own custom EULAs instead—subject to a few caveats, as mentioned in our fifth item below. Because the default EULAs can be quite limited and can't possibly address the unique issues that any particular app is likely to raise, a company should ideally adopt its own EULA to best protect its interests in its apps.

2. Is Your EULA Binding?

The best EULA is a binding EULA. U.S. courts have consistently made clear that a "clickwrap"-style agreement has the best chance of being enforceable; although whether an agreement is enforceable in any particular case may depend on how the agreement is actually presented to users and how users indicate their assent. Having adopted customized EULAs, companies have several opportunities to present their EULAs to users. In most app stores, for example, a dedicated link called "License Agreement" lets companies link to their EULAs. In addition, companies should ideally include language in their apps' "Description" field making clear to users that, by downloading and using the app, they are accepting the EULA. But it's still possible in most app stores for users to purchase and download an app without seeing the EULA; accordingly, for apps that may present significant risk issues—such as banking or e-commerce apps—the most conservative approach is to require an affirmative "click-accept" of the EULA when the app is first opened by a user on his or her device.

3. Which Parties Will Your EULA Bind?

If an app is targeted toward businesses, or toward individuals who will use the app in their business capacities, then the EULA should ideally bind both the individual who uses the app and the individual's employer. Similarly, if minors will be permitted to use the app, then the EULA should require that a parent or guardian consent on the minor's behalf. (Of course, if minors under 13 will be allowed to use the app, or if the app will be directed toward such minors, you will need to address Children's Online Privacy Protection Act issues in connection with the app.)

4. Where Will Your EULA Reside?

As a technical matter, a EULA can reside in one of two places: it can be "hard-coded" into the app itself, so that the EULA is downloaded together with the app, or it can reside on a separate web server maintained by the developer. The former approach ensures that the EULA is always accessible to the user, even if the user's device is offline. Some users may decide not to download the latest updates, however, and, as a result, those users may not be bound by the updated terms. In contrast, under the latter approach, companies can update their EULAs at any time by simply updating the document on their own web servers, although the EULAs won't be available to the user offline. Companies should think about which approach works best for their specific apps and their associated risk issues.

5. Does Your EULA Incorporate Terms Required by Third Parties?

Some app stores, such as the Apple App Store, understandably require that, if a company adopts a custom EULA for its app, such customized EULA must include terms protecting the applicable app store owner. (Other app stores, such as the Amazon Appstore for Android, place such protective terms in their own user-facing agreements and require developers to acknowledge that such protective terms will govern.) Other third-party terms may also apply, depending on any third-party functionalities or open-source code incorporated into the app. For example, if a company integrates Google Maps into its app, Google requires the integrating company to pass certain terms on to its end users. The licensors of any open-source code used by an app may also require the company to include certain disclaimers, attributions, usage restrictions or other terms in the EULA.

6. Is your EULA clearly written and reasonable?

Traditionally, EULAs have been overlong, filled with impenetrable legal jargon and, frankly, hard to read, sometimes even for lawyers. An emerging best practice, especially for B2C apps, is to draft app EULAs that are understandable to consumers and to minimize unnecessary legalisms such as "null and void," "including without limitation" and the reflexive prefacing of sentences with "we hereby reserve the right" or "you hereby acknowledge and agree." Moreover, because space on a mobile device screen can be limited, thought should be given to eliminating repetition in app EULAs wherever possible. Of course, even if a EULA is written in plain English, extremely one-sided provisions—such as a disclaimer of direct damages (rather than a cap on such damages)—may raise concerns with a court in any subsequent litigation involving the EULA. At the same time, the EULA is ultimately a legal document, and an app developer will want to make sure that any slimmed-down or simplified EULA still provides adequate protection for the developer.

Of course, if you collect personal information through your mobile app, you'll also need to have a privacy policy in place—but that's a topic for another article!

"NEVER SAY NEVER": LESSONS FROM RADIOSHACK'S SALE OF CUSTOMER INFORMATION

By G. Larry Engel and Kristin A. Hiensch

When a bankrupt company's most valuable assets include consumer information, a tension arises between bankruptcy policy aimed at maximizing asset value, on the one hand, and privacy laws designed to protect consumers' personal information, on the other. Such tension played out recently in the Chapter 11 bankruptcy case of RadioShack, where the bankrupt retailer's attempt to sell customer data invoked objections from 38 state attorneys general, the Federal Trade Commission (FTC) and others who claimed the sale would violate RadioShack's stated privacy policy of never selling customers' personal information. These issues are not new.

CONSUMER DATA IN DOT COM ERA—TOYSMART

Back in the dot-com era, online toy retailer Toysmart sought bankruptcy court approval to sell customer data. Toysmart's privacy policy expressly told customers that they could "rest assured" that their information would "never be shared with a third party." Nevertheless, once it ceased operations and entered bankruptcy in May 2000, Toysmart solicited bids for the sale of such personal information, including its customers' names, addresses, billing information, shopping preferences and family profile information. The FTC opposed the sale, arguing that the breaking of the promise to never share information would be deceptive, in violation of Section 5 of the FTC Act.

The FTC and Toysmart reached a deal that, along with other restrictions, would limit the sale of customer data to a family-friendly company that would agree to be bound by Toysmart's privacy policy. Even so, 46 states objected to such a resolution, arguing that any sale of customer data that did not provide an opt-out for customers would violate Toysmart's privacy policy and, as such, would constitute an unfair or deceptive business practice, in violation of state "little FTC Acts." Ultimately, Toysmart withdrew the customer information from the auction and destroyed it.

RADIOSHACK—FOLLOWING THE TOYSMART EXAMPLE

RadioShack's sale process replayed several of the Toysmart themes and similarly met a negotiated—not judicially determined—resolution. Following the sale of its 1,743 store leases this spring to General Wireless, an affiliate of hedge fund Standard General, RadioShack initiated an auction process for the sale of its intellectual property, including the RadioShack name and a collection of customer information.

> The main lesson from RadioShack is this: privacy policies ideally should anticipate bankruptcy scenarios and alert consumers that their information may be sold in bankruptcy or other divestitures.

During the course of its long tenure as a consumer electronics retailer, RadioShack collected names, email addresses, physical addresses, telephone numbers, credit card numbers and purchase history data for over 117 million customers. All such information had been collected under a privacy policy that promised RadioShack would "not sell or rent your personally identifiable information to anyone at any time." Indeed, in a privacy policy on display in RadioShack's retail stores, the company noted: "We pride ourselves on not selling our private mailing list."

RadioShack's customer information, however, is a valuable asset. Accordingly, as part of the bankruptcy process, the RadioShack trustee sought court approval to sell a subset of such

information in its database, including 67 million complete customer names and physical addresses, and approximately 8.3 million email addresses, to General Wireless for $26.2 million dollars.

The proposed sale drew objections from state attorneys general, the FTC and companies such as AT&T and Verizon. Fundamentally, the FTC and state objectors argued that the sale would contradict RadioShack's privacy policy and, as such, would constitute a deceptive business practice. AT&T, Verizon and others asserted that the sale would violate the agreements signed between RadioShack and each of the objectors, as well as RadioShack's own privacy policy.

The debtor and various objectors mediated these issues and ultimately reached a deal modeled on the Toysmart approach. In the end, Bankruptcy Court Judge Brendan L. Shannon approved the parties' settlement, authorizing the sale subject to certain conditions, including that General Wireless must:

- Send emails to all included email addresses notifying customers of the purchase and offering them seven days to opt-out of the transfer of their personal information;
- Mail those customers for whom it has a physical address, but no email address, a notification that it has purchased the assets of RadioShack and offering such customers 30 days to opt-out of the transfer of their information;
- Provide a notice on the RadioShack website, with both an online opt-out option and a toll-free telephone number to call to exercise the option; and
- Agree to be bound by the existing RadioShack privacy policy with regard to purchased customer information.

Furthermore, the deal prohibits RadioShack from transferring sensitive information, such as debit or credit card numbers, dates of birth, Social Security numbers or other government-issued identification numbers.

COMMENTARY

In the intervening 15 years since the Toysmart brouhaha, very little legal guidance has developed to define the contours of pre-bankruptcy privacy promises in bankruptcy sales. As in the Toysmart situation, the privacy-related objections raised to the RadioShack sale were consensually resolved, leaving parties without a judicial resolution to these issues. Nevertheless, certain themes are emerging.

First, by virtue of settling, the FTC and states seem to recognize that consumer privacy rights are not absolute—they must be balanced with the best interests of a debtor's estate and creditors in bankruptcy.

Second, a theme in both settlements is honoring consumers' original expectations—that is, requiring the purchaser to adopt the privacy policy in place at the time the information was collected.

Third, the ability for customers to opt-out of the transfer of their personal information seems to be key. This was a sticking point in the Toysmart matter, leading to the ongoing controversy even after resolution with the FTC.

More broadly, however, perhaps the main lesson from RadioShack is this: Privacy policies ideally should anticipate bankruptcy scenarios and alert consumers that their information may be sold in bankruptcy or other divestitures. Such a direct acknowledgement would serve consumers by advising them of the possible fate of their personal information, thereby allowing them to make an informed decision about what information to volunteer. It would also serve the eventual debtor and its creditors, simplifying the sale process and maximizing the sale value of collected information.

FEDERAL DISTRICT COURT: "BROWSEWRAP" TERMS AND CONDITIONS PROVIDE SUFFICIENT NOTICE TO DEFEAT FALSE ADVERTISING CLASS ACTION

By Duane L. Carver, Jr. and Aaron P. Rubin

Websites sometimes present their terms of use ("TOU") to users merely by including a link to those TOU on the website without requiring users to affirmatively accept the terms by, for example, checking a box or clicking an "I accept" button. As we have written previously, Courts tend to look disfavorably on such website TOU presentations, which have become somewhat misleadingly known as "browsewrap agreements," when determining whether a TOU constitutes an enforceable contract between the website operator and a user. According to a recent federal district court opinion, however, browsewrap TOU might be sufficient to help websites achieve another legal end: providing sufficient notice to defeat a false advertising claim based on an allegedly fraudulent omission.

In the case *Handy v. LogMeIn, Inc.*, the U.S. District Court for the Eastern District of California held that a software vendor's online terms and conditions provided notice that the company might discontinue its app, and that such notice was sufficient to defeat a customer's claims under California's false advertising and unfair competition laws *regardless of whether the customer had affirmatively accepted the TOU*.

The defendant, LogMeIn, Inc., sells software for accessing computer files remotely from separate computers or mobile devices. LogMeIn previously provided its software as two separate products: LogMeInFree, a free service that allowed users to log into remote computers from a desktop or laptop; and Ignition, a paid service that allowed users to log into computers using mobile devices. Before 2011, the plaintiff, Darren Handy, downloaded LogMeInFree and then paid for Ignition. In 2014, LogMeIn introduced a new paid product called "LogMeInPro," which merged the features of LogMeInFree and Ignition. Eventually, LogMeIn posted a message on its website stating it would begin migrating users of LogMeInFree and Ignition to the new platform while ending support and maintenance on the older platforms. This required users of LogMeInFree and Ignition to pay for LogMeInPro in order to receive continued support and maintenance for Ignition and to continue to use the functionality previously provided for free as part of LogMeInFree.

Even if a browsewrap does not constitute a contract, it may serve a useful purpose by providing legally significant notices to users.

In response, Mr. Handy brought a class action suit alleging he would never have purchased Ignition if he had known that the company would discontinue support for Ignition or require additional payment for continued access to the LogMeInFree functionality. His suit claimed that LogMeIn violated California Business and Professions Code §§ 17200 and 17500 by fraudulently failing to disclose that the company might discontinue support and change its pricing model for the software. LogMeIn argued, among other things, that its online TOU reserved the right for LogMeIn "to modify or discontinue any Product for any reason or no reason." But Handy argued that this statement was not binding on him because he never affirmatively accepted the TOU.

The court disagreed, however, holding that "whether the Terms and Conditions constituted an enforceable contract is irrelevant to whether the Terms and Conditions related to LogMeInFree provided notice to prospective purchasers of the Ignition app that LogMeInFree could be discontinued." The court went on to note that, while LogMeIn's TOU may not have been "forced on Plaintiff through a clickwrap," the TOU nonetheless showed that LogMeIn had "publish[ed] the fact that it reserved the right to terminate the free app, LogMeInFree." Therefore, the court held that there was "an insufficient showing that information related to the future termination of LogMeInFree constituted a material omission when selling the Ignition app."

Clients often ask us whether a "browsewrap" TOU serves any purpose at all, given the fact that courts are often disinclined to construe such TOU presentations as creating an enforceable contract. *Handy v. LogMeIn, Inc.* shows that, in at least some circumstances, the answer is yes; even if a browsewrap does not constitute a contract, it may serve a useful purpose by providing legally significant notices to users.

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

By Melissa M. Crespo and Christine E. Lyon

A recent survey of hiring managers and human resource professionals reports that more than 43 percent of employers use social networking sites to research job candidates. This interest in social networking does not end when the candidate is hired; to the contrary, companies are seeking to leverage the personal social media networks of their existing employees, including for their own marketing purposes, as well as to inspect personal social media in workplace investigations. As employer social media practices continue to evolve, individuals and privacy advocacy groups have grown increasingly concerned about employers intruding upon applicants' or employees' privacy by viewing restricted-access social media accounts.

Although federal legislation has been proposed several times (see here and here), efforts to enact a national social media privacy law have not been successful. In the absence of such legislation, states are actively seeking to address employee social media privacy issues. In 2014, six states passed social media laws, and, since the beginning of 2015, four more states have passed or expanded their social media laws. Similar legislation is pending in at least eight more states. In total, 22 states have now passed special laws restricting employer access to personal social media accounts of applicants and employees ("state social media laws").

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

KEY RESTRICTIONS UNDER STATE SOCIAL MEDIA LAWS

As a general matter, these state social media laws bar employers from requiring or even "requesting" that an applicant or employee (21 of the 22 state laws protect both current employees and applicants; New Mexico's law protects

only applicants) disclose the user name or password to his or her personal social media account. Some of these state laws also impose other express restrictions, such as prohibiting an employer from requiring or requesting that an applicant or employee:

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

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

For example, a few states, like New Mexico, only cover traditional social networking accounts, while most other state laws broadly apply to any electronic medium or service that allows users to create, share or view user-generated content, including videos, photographs, blogs, podcasts, messages, emails and website profiles generally. Some of these laws only prohibit employers from seeking passwords or other login credentials to personal social media accounts, while other states impose the broader restrictions described above. For example, Arkansas, Colorado, Oregon and Washington prohibit an employer from requesting that an employee allow the employer access to his or her personal social media accounts; and California, Connecticut, Oklahoma, Michigan, Rhode Island, Tennessee and Washington prohibit an employer from requesting an employee to access his or her personal account in the presence of the employer. Certain states prohibit an employer from requiring an employee to change his or her privacy settings to allow the employer access to his or her private social media accounts, although it is possible that such a restriction might be inferred from at least some of the other state laws as well. Even more confusing are the inconsistencies across state laws with respect to exceptions for workplace investigations, as discussed below.

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

Employers must evaluate their current practices and policies to ensure compliance with state laws.

WHAT EVERY EMPLOYER SHOULD KNOW ABOUT STATE SOCIAL MEDIA LAWS

A. Applicant Screening

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

Additionally, most of these laws explicitly state that they do not prohibit viewing information about an applicant that is available to the public. For example, the Michigan law "does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain."All of these state social media laws, however, prohibit employers from seeking access to the nonpublic social media pages of applicants. In practice, this means that employers should avoid asking applicants about the existence of their personal social media accounts and requesting, or even suggesting, that an applicant friend the employer or a third party, including a company that provides applicant background investigations.

B. Friend Requests

Certain laws expressly restrict an employer's ability to encourage an employee to friend or add anyone to the list of contacts for his or her personal social media accounts. This may include, but is not limited to, the employer, its agents, supervisors or other employees.

For example, Colorado's social media legislation states that an employer shall not "compel an employee or applicant to add *anyone,* including the employer or his or her agent, to the employee's or applicant's list of contacts associated with a social media account," and many other laws contain this type of prohibition against requesting access via what may be intended as a harmless friend request.

Although these laws do not prohibit a subordinate from friending a manager or supervisor, employers should exercise care not to require, or even request or encourage, employees to friend supervisors or other company representatives. Employers in states without social media laws or states with laws that allow "friending" should nevertheless proceed with caution when requesting access to an employee's or applicant's personal social media pages and think twice about "friending" or "following" employees. If an employer learns about an employee's legally protected characteristic (such as religion, pregnancy, medical condition

or family medical history) or legally protected activity (such as political or labor union activity), the employer may face greater exposure to discrimination claims if it later takes adverse action against the employee.

These restrictions may be particularly significant for employers seeking to leverage employees' personal social media connections for work-related marketing or business development purposes. Employers should be aware that, even in states without an express restriction on friend requests, a law that generally prohibits an employer from attempting to access an employee's or applicant's social media account may effectively limit an employer's ability to require or encourage employees to friend people.

C. Account Creation and Advertising

Recently, Oregon amended its existing social media law to prohibit categories of employer conduct not previously addressed in any of the existing social media laws. Under the new amendment (which takes effect on January 1, 2016), employers are prohibited from requiring or requesting that an applicant or employee establish or maintain a personal social media account or that an applicant or employee authorize the employer to advertise on his or her personal social media account. Notably, the Virginia law, which went into effect July 1, 2015, implies that an employer may be permitted to engage in the type of conduct the Oregon law seeks to prevent. The Virginia law explicitly excludes from covered information an account set up by the employee at the request of the employer.

D. Investigations

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

No express exception for investigations: The Illinois and Nevada social media laws do not provide any express exception for workplace investigations that might require access to an employee's personal social media accounts. This suggests that an employer's investigation of potential misconduct or legal violations may not justify requesting or requiring an employee to disclose his or her social media login credentials. (We note that, perhaps in an effort to broaden employer investigation efforts and clarify an existing ambiguity, Illinois amended its law so that, where the access sought by the employer relates to a professional account, an employer is not restricted from complying with a duty to screen employees or applicants, or to monitor or retain employee communications as required by law.)

Limited exception for investigations of legal violations: California's social media law provides that it does not limit an employer's ability to request that an employee divulge personal social media in connection with an investigation of employee violations of applicable laws. However, this exception does not appear to extend to other prohibited activities, such as asking an employee to disclose his or her user name and password for a personal social media account. Other states provide exceptions only for investigations of specific types of legal violations. For example, the Colorado and Maryland social media laws only provide an exception for investigating violations of securities laws or potential misappropriation of proprietary information.

Limited exception for misconduct investigations: Some social media laws extend the exception beyond investigations of legal violations to investigations of alleged misconduct. These states include California, Oregon and Washington. In general, these laws allow an employer to ask an employee to divulge content from a personal social media account, but still do not allow the employer to request the employee's login credentials. In contrast, some states, including Arkansas, Colorado, Maryland and Michigan permit an employer to request any employee's social media login credentials to investigate workplace misconduct.

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

E. Best Practices

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

Review hiring practices for compliance with social media laws: Employers should ensure that all employees involved in the hiring process are aware of the restrictions imposed by these state social media laws. For example, recruiters and hiring managers should refrain from inquiring about an applicant's personal social media pages or requesting access to such pages. While these state social media laws do not prohibit employers from

accessing publicly available personal social media sites, employers will also want to evaluate whether this practice is advisable, given the risk of stumbling across legally protected information that cannot be used in employment decisions.

Implement social media guidelines: Employers should implement social media guidelines to mitigate potential risks posed by employee social media postings, being mindful of restrictions arising under the National Labor Relations Act and other federal and state laws. Employers also should ensure that their social media guidelines do not run afoul of these state social media laws.

Educate and train personnel: Personnel involved in internal investigations, such as human resources and internal audit personnel, need to be aware of the growing restrictions on employer access to employee personal social media accounts. Prior to seeking access to an employee's personal social media accounts, or content from such accounts, the internal investigators should check any applicable restrictions. In general, given the general trends in these laws, employers should avoid requesting login credentials to employees' personal social media accounts, even in the context of investigation, unless they have first consulted legal counsel.

WASHINGTON STATE COURT REFUSES TO UNMASK ANONYMOUS ONLINE REVIEWER

By Aaron P. Rubin

In a precedent-setting ruling, the Washington Court of Appeals in *Thomson v. Doe* refused to grant a motion to compel brought by a defamation plaintiff who had subpoenaed the lawyer-review site Avvo.com seeking the identity of an anonymous online reviewer, holding that, for a defamation plaintiff to unmask an anonymous defendant, that "plaintiff must do more than simply plead his case."

When deciding whether to require disclosure of an anonymous speaker's identity, the nature of the speech at issue should inform the choice of evidentiary standard.

The plaintiff in the case, Florida divorce attorney Deborah Thomson, filed a defamation suit against an anonymous poster of Avvo reviews. Claiming to be a former client, the reviewer stated that Thomson, among other things, failed to live up to her fiduciary duties, failed to subpoena critical documents and failed to adequately represent the reviewer's interests.

After Avvo refused Thomson's subpoena seeking the anonymous reviewer's identity, Thomson moved to compel compliance with the subpoena. The Washington State trial court denied Thomson's motion and she appealed, presenting the Washington State Court of Appeals with what the court acknowledged was an issue of first impression in the Evergreen state: What evidentiary standard should a court apply when deciding a defamation plaintiff's motion to reveal an anonymous speaker's identity?

The court began its analysis by describing the holdings of the two leading cases on the issue: New Jersey's *Dendrite Int'l, Inc. v. Doe No. 3*, which held that, to unmask anonymous defendants in defamation cases, the plaintiff must "produce sufficient evidence supporting each element of its cause of action on a prima facie basis; and Delaware's *Doe v. Cahill*, which established that plaintiffs seeking to uncover the identities of anonymous speakers/defendants must clear a slightly higher evidentiary threshold—proof that their claims would survive a summary judgment motion.

The court also discussed the one court that "has significantly strayed from *Dendrite and Cahill*": the Virginia Court of Appeals. In *Yelp, Inc. v. Hadeed Carpet*, another case we recently covered at *Socially Aware*, the Virginia Court of Appeals "declined to adopt either test, instead applying a state statute that required a lower standard of proof." Specifically, *Hadeed* held that, in the *Thomson* court's words, "a defamation plaintiff seeking an anonymous speaker's identity must establish a good faith basis to contend that the speaker committed defamation."

The *Thomson* court then cited, with approval, the Ninth Circuit's approach in *In re Anonymous Online Speakers*. In that case, the Ninth Circuit determined that, when deciding whether to require disclosure of an anonymous speaker's identity, the nature of the speech at issue should inform the choice of evidentiary standard. Holding that an online review of an attorney's services is not merely commercial speech—which, the court explained, would warrant the lowest level of protection—the court rejected the *Hadeed* (good faith) standard. Since the Avvo review did not qualify as political speech either, the court also discounted the highest level of protection. The court then determined that the "motion to dismiss standard" was "inadequate to protect this level of speech" because, in a notice pleading state like Washington, "a defamation plaintiff would need only to allege the elements of the claim, without supporting evidence."

Finally, the *Thomson* court addressed the "two remaining standards": prima facie (*Dendrite*) and summary judgment (*Cahill*). The court ultimately decided that the prima facie standard was appropriate because the anonymous reviewer had yet to appear in the case

and the plaintiff, therefore, was not in a position to file a summary judgment motion.

The court nevertheless observed that "the important feature" of both the prima facie and the summary judgment standards "is to emphasize that the plaintiff must do more than simply plead his case." In other words, both standards require "supporting evidence ... before the speaker is unmasked." Under that standard, the court held, "Thomson's motion must fail. As Thomson freely admits, she presented no evidence to support her motion."

"NOTES" UPDATE SHOWS FACEBOOK'S CONTINUED EFFORTS TO INCREASE ALREADY IMPRESSIVE USER ENGAGEMENT

By Aaron P. Rubin

As the number of social media platforms continues to grow, users' online activity is becoming increasingly divided, requiring social media companies to prove to potential advertisers that they not only have a lot of registered users, but that those users are engaged and spending a lot of time on their platforms.

Having accumulated nearly 230 billion minutes of user-time, Facebook is several lengths ahead of the competition in the user engagement race; its users have spent 18 times more time on the platform than users of the next-biggest social network, Instagram (which, of course, is owned by Facebook). Despite its clear lead, Facebook seems to be keeping user engagement at the top of its priority list, introducing features that reduce its users' need to access resources outside the Facebook ecosystem.

Take, for example, Facebook's introduction of "native video." Native videos are videos that are posted directly to Facebook rather than first being uploaded to another site such as YouTube and then shared on Facebook as links. Native videos on Facebook have been shown to significantly outperform videos shared on Facebook from other sites in terms of engagement.

By testing an update of its "Notes" feature, Facebook may be indicating a desire to keep its users from venturing off the platform to use third-party blogging platforms and personal websites.

A Facebook feature known as auto-play further increases user engagement by ensuring that Facebook native videos—and only Facebook native videos—automatically play as users scroll down their newsfeeds. After one quarter with the auto-play in place, Facebook experienced a 58% increase in engagement.

Now, by testing an update of its "Notes" feature, Facebook may be indicating a desire to keep its users from venturing off the platform to use third-party blogging platforms and personal websites, too.

Before 2011, when Facebook statuses were limited to 500 characters, the Notes feature allowed Facebook users to create longer posts that, like their photo albums and favorite book choices, would always be attached to their profiles. Since Facebook has significantly loosened up its character limits, the purpose of Notes has been unclear.

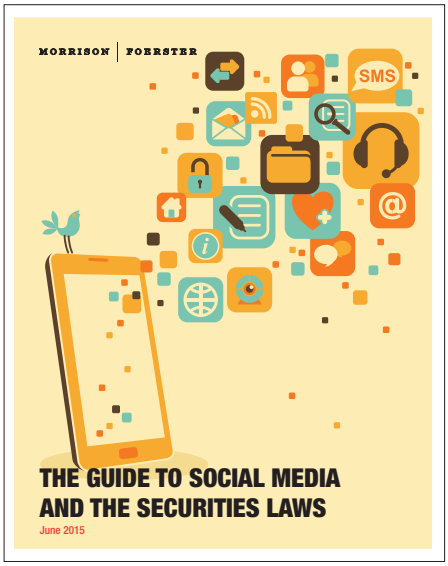
But Facebook recently updated Notes to allow users to create posts with a more sophisticated look and an accompanying picture. The updated Notes feature was described by a Facebook spokesperson as the company's attempt "to make it easier for people to create and read longer-form stories on Facebook." Some social media industry observers have suggested that this update is intended to provide users with an alternative to Medium, a blogging platform favored by those in the technology and media industries.

"But that might be too early an assessment," writes *Motherboard*'s Clinton Nguyen, "as [the new Notes feature is] a work in progress, the revamp is only available for a handful of users."

Nguyen is right; it's too early to tell whether social media enthusiasts will want to create and read lengthy personal essays on Facebook. One thing *is* for sure, however: Facebook is not letting up on its efforts to remain the user-engagement king.

THE GUIDE TO SOCIAL MEDIA AND SECURITIES LAW

By Jay Baris and David M. Lynn



The growing use of social media has created challenges for federal securities regulators and, given the significance of social media as a preferred method of communication for a large percentage of market participants, the need to adapt Federal securities laws and the regulatory framework applicable to broker-dealers and investment advisers to social media channels has become all the more urgent.

To help navigate these issues, *Socially Aware* contributors and Morrison & Foerster partners Jay Baris and David Lynn have recently released their Guide to Social Media and Securities Law, which provides a comprehensive overview of how federal regulation of securities has evolved in the face of the growing use of social media by investors, securities issuers, broker-dealers, investment advisers and investment companies.

The guide is now available here. We think that you will find it to be a terrific resource.

If you wish to receive a free subscription to our Socially Aware newsletter, please send a request via email to **sociallyaware@mofo.com**. We also cover social media-related business and legal developments on our Socially Aware blog, located at **www.sociallyawareblog.com**.

For breaking news related to social media law, follow us on Twitter **@MoFoSocMedia**. To review earlier issues of Socially Aware, visit us at **www.mofo.com/sociallyaware**.