Volume 6, Issue 3, July/August 2015

SOCIALLY AWARE

THE BURTON AWARDS
2011 BEST LAW FIRM NEWSLETTER

THE SOCIAL MEDIA LAW UPDATE

IN THIS ISSUE

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 present a "grand unifying theory" of today's leading technologies and the legal challenges these technologies raise; we discuss whether hashtags can be protected under trademark law; we explore the status of social media accounts in bankruptcy; we examine the growing tensions between content owners and users of livestreaming apps like Meerkat and Periscope; we highlight a recent discovery dispute involving a deactivated Facebook account; we discuss a bill before Congress that would protect consumers' rights to post negative reviews on websites like Yelp; and we take a look at the Federal Trade Commission's crackdown on in-store tracking activities.

All this—plus an infographic exploring the popularity of livestreaming sites Meerkat and Periscope.

EDITORS

John F. Delaney
Aaron P. Rubin

CONTRIBUTORS

John F. Delaney
G. Larry Engel
Adam J. Fleisher
J. Alexander Lawrence
David F. McDowell
Julie O'Neill
Vincent J. Novak
Jake Joseph Perkowski
Dina Roumiantseva
Aaron P. Rubin
Cara Ann Marr Rydbeck
Michael Wawszczak

FOLLOW US

Morrison & Foerster's Socially Aware Blog

@MoFoSocMedia

MORRISON FOERSTER

TOWARD A GRAND UNIFYING THEORY OF TODAY'S TECH TRENDS

By John F. Delaney

As a technology law blogger and co-editor of *Socially Aware*, I monitor emerging developments in information technology. What's hot in IT today? Any shortlist would have to include social media, mobile, wearable technology, the Internet of Things (IoT), cloud computing and big data.

That list is all over the map, right? Or is it? On closer inspection, these technologies are far more closely intertwined than they may appear to be at first glance.

So what's the connection between, say, social media and the IoT? Or wearable tech and cloud computing?

Here's my theory: These technologies all reflect the ceaseless drive by businesses to collect, store and exploit ever more data about their customers. In short, these technologies are ultimately about selling more stuff to us.

With this "grand unifying theory" in mind, one sees how these seemingly disparate technologies complement one another. And the legal challenges and risks they pose become clear.

COLLECTION OF DATA

Let's start with the collection of consumer data. Of the six key trends identified above, four relate directly to such collection: social media, mobile, wearable technology and IoT.

When we use the Internet, marketers are tracking our activities; the data generated by our online behavior is collected and then used to target ads that will be more relevant to us.

If we spend time on movie sites, we're more likely to see ads promoting new film releases. If we visit food blogs, we're going to be served ads selling cookware.

Creepy? It can be. But such tracking and targeting make it possible for many website operators to offer online content and services for free. Indeed, many believe that such tracking and targeting are essential to the vibrancy of our Internet ecosystem. (Although Google is reportedly experimenting with an offering where one would pay not to see ads while surfing the Web.)

> From a marketer's perspective, social media and mobile are all about expanding the amount and type of customer data that can be collected.

In the past, serious limitations existed on the ability of marketers to track and target us. We might have given our name, email and home address to a website, but not much else; now, with social media, we routinely volunteer loads of personal information—our jobs, hobbies, special skills, taste in music and movies, even our "relationship status." And not just information about ourselves, but our families, friends and colleagues as well. As a result, social media companies have compiled huge databases about us—in Facebook's case, nearly 1.4 billion of us.

Also, not long ago, we surfed the Web from either home or office—limiting the ability to be tracked and targeted while away from those locations. The rise of Internet-connected mobile devices has changed all that, of course—now we can access the Web from anywhere, and mobile devices can pinpoint our location, even when we're not browsing. Marketers can track our daily journey to and from home to work and back again, even serving us "just in time" discount offers as we pass a clothing store or restaurant.

From a marketer's perspective, social media and mobile are all about expanding the amount and type of customer data that can be collected. Thanks to mobile devices and apps, tracking and targeting are no longer desk-bound and can occur even if a customer is not connected to the Internet.

Wearable tech? Like cell phones, wearables make tracking and targeting possible while one is away from a traditional computer or not actively using the Web. These devices can also collect information that cell phones can't—our heart rate or body temperature, or the number of hours one slept last week.

For marketers, the IoT is especially exciting because it raises the possibility of being able to track and target consumers anywhere in their homes, even while they are away from their desktop computers or mobile devices.

Imagine your "smart" refrigerator not only determining when you're low on milk, but offering a 15 percent discount if you were to buy a quart of milk today at your local market. Or your Internet-connected washing machine recommending a new laundry detergent based on its monitoring of your laundry loads.

Another hot technology trend—commercial drones—is relevant here. Although unmanned aerial vehicles (UAVs) have generated attention for their ability to facilitate package delivery and accommodate WiFi access, they can be used to collect data on consumers when they're outdoors or near a window, even when they are without cell phones, wearables or other devices used to track their movement and activities.

Ingestibles—"smart" pills containing sensors that are swallowed, allowing the collection of data *within one's body*—

HAS LIVESTREAMING CAUGHT ON YET?

The livestreaming apps Meerkat and Periscope are the talk of the tech world, but does the general population know anything about them? Let's see what the stats say…

Number of users Meerkat acquired within 49 days of launch: **700,000** [1]

Percentage of U.S. Internet users who have heard of Meerkat: **9%**[3]

Percentage of Meerkat users who watch more than 2 hours of live video a day: **20%** [4]

Most popular Meerkat Stream: **SXSW KEYNOTE WITH JACK WELCH** (2,261 views) [5]

Length of time it took one person to build Meerkat: **8 WEEKS** [6]

Number of users Periscope acquired within 10 days of launch: **1 MILLION** [2]

Percentage of U.S. Internet users who have heard of Periscope: **6%** [3]

SOURCES

1. http://blog.hubspot.com/marketing/meerkat-growth-show
2. http://www.theverge.com/2015/4/28/8510841/periscope-1-million-users-in-first-10-days
3. http://www.emarketer.com/Article/Consumers-Streaming-Periscope-Meerkat/1012562?ecid=SOC1001
4. http://mashable.com/2015/03/15/meerkat-2hours-video-daily/
5. http://simplymeasured.com/blog/2015/03/16/91000-meerkats-how-many-popped-up-at-sxsw/#i.q0c2e8zlhd42zg
6. http://venturebeat.com/2015/03/13/twitter-cripples-meerkat-by-cutting-off-access-to-its-social-graph/

are a nascent technology that, as they become more widely used, may ultimately fit into this theory.

STORAGE OF DATA

With social media platforms, mobile, wearable and IoT devices and UAVs collecting information on an unprecedented scale, that data needs to be stored somewhere. Enter the cloud. All of these new technologies depend heavily on the massive storage capacity made possible by cloud systems; it wouldn't be cost effective otherwise. (Case in point: A 2013 study revealed that 90% of all the data in the world had been collected over the prior two years.)

EXPLOITATION OF DATA

Once all of this data has been collected and stored in the cloud, what then?

That's where big data enters the picture. Big data is providing companies with the analytic tools for sifting through these inconceivably large databases in order to exploit the bits therein.

For example, that photo you uploaded to Instagram can now be analyzed for marketing opportunities. Perhaps you were holding a bag of potato chips; using big data analytics, the chip maker could target you in its next online ad campaign. Or maybe a competing snack company wants to entice you to switch brands. Why stop there? What about the shirt that you were wearing? And that pair of jeans? (I've written on the application of big data analytics to the billions of photos hosted on social media sites here.)

Similarly, information collected from wearables, when processed by big data tools, opens up new opportunities for marketers. Your pulse rate may be of interest to the health care industry. Your jogging workouts may attract attention from retailers of athletic shoes and clothing.

But the mother lode just might be all of the marketing insights to be generated by big data analytics stemming from multiple IoT devices in one's home—the thermostat, stove, refrigerator, coffee machine, toaster, washer/dryer, humidifier, alarm clock and so on: for the first time ever, marketers will have access to real-time information regarding once-private quotidian activities.

LEGAL CONSIDERATIONS

So that's my theory: The adoption of today's hottest IT technologies is being driven in large part by the insatiable desire of businesses to collect and store ever-larger amounts of consumer data, and to then use that data to more successfully market to consumers. When these technologies are viewed in light of this theory, some key legal observations emerge.

First, because these technologies all involve the collection, storage and exploitation of consumer data, privacy and data security are necessarily raised and indeed are the most important legal considerations. That's not meant to minimize intellectual property, product liability and other legal concerns associated with these technologies; privacy and data security laws, however, are the ones specifically designed to regulate the collection, use and exploitation of consumer data.

Second, these technologies are being developed and implemented far faster than the ability of legislators, regulators and courts to develop rules to govern them. It will be essential for companies embracing these technologies to self-regulate—failure to do so will result in an inevitable backlash, leading to burdensome regulations that will undermine innovation.

Third, these technologies will present real challenges to the majority of companies that want to "do the right thing" by their customers. For example, consumers ideally should be provided with notice and an opportunity to consent prior to the collection, storage and exploitation of their personal information, but how can this be done through, say, a smart electric toothbrush? These issues need to be addressed early in the development cycle for next-generation products—it can't be an afterthought. Moreover, are customers receiving real, tangible value in connection with the data being collected from them?

Fourth, as our social-media pages, devices and appliances become more closely tied together, and linked to massive troves of data about us in the cloud, businesses need to be aware that it takes only one weak link to put the entire ecosystem at risk. Hackers will no longer need to bypass your computer or phone's security to capture personal data; they may be able to access your records through, say, an Internet-enabled toaster that lacks adequate security controls.

Finally, companies need to pay attention to whether they need to collect all the data that can be collected through these technologies. Ideally, they should seek to minimize the amounts of personally identifiable information they hold, in order to reduce privacy- and security-related legal risks and liability.

> **It will be essential for companies embracing these technologies to self-regulate – failure to do so will result in an inevitable backlash.**

No doubt this last recommendation may be hard for many marketers to embrace; after all, data gathering is in their DNA. And that same hard-wiring is in all of our DNA—the original source code for data collection, storage and exploitation. We wouldn't be human without it.

(This is an expanded, "director's cut" version of an op-ed piece that originally appeared in MarketWatch.)

#TRADEMARKS?: HASHTAGS AS TRADEMARKS

By Dina Roumiantseva and Aaron P. Rubin

Hashtags have become ubiquitous in social media, but their status as intellectual property—particularly as trademarks—is still developing. First adopted by Twitter users to link user posts, hashtags are character strings preceded by the "#" symbol that generate a link to all other posts containing the same tag. Today, in addition to providing the search-related functionality for which they were first developed, hashtags provide businesses new ways to engage with consumers. Hashtag marketing campaigns by businesses generate brand awareness by encouraging social media users to post with the campaign tag and, in return, offer users discounts, prizes or even a chance to become a model.

But can a hashtag be registered as a trademark? The functional nature of hashtags led to initial uncertainty on this question, which the U.S. Patent and Trademark Office (USPTO) settled in 2013 when it added a new section to the Trademark Manual of Examination Procedure on registration of hashtag marks. The USPTO defines a hashtag as "a form of metadata comprised of a word or phrase prefixed with the symbol '#'" and states that a hashtag mark may be registerable, but only if it functions as an identifier of the source of the applicant's goods or services. For example, #ingenuity would be registerable for business consulting services as a distinctive term, while #skater for skateboard equipment would be merely generic and non-registerable. In addition, to obtain a registration, the applicant must provide evidence of the use of the mark in connection with the relevant goods or services, which means that, like any other trademark, a hashtag mark must actually be used in commerce to be registrable.

Unlike traditional tag lines, which are meant to be used primarily by the mark owner, hashtags are typically intended to be disseminated by social media users. For example, the makers of Mucinex have registered #blamemucus, which allows potential consumers to commiserate about their colds through social media, as well as spread the word about Mucinex and participate in drawings for prizes. The #blamemucus registration covers both the pharmaceutical products themselves (with a store display bearing the mark as a specimen of use) and services consisting of providing information in the field of respiratory and pulmonary conditions via the Internet (with the company website as a specimen). By covering both the core goods and online services, the registration provides broad protection for the hashtag mark against use by competitors. Companies may also attempt to register a phrase that has already become an Internet meme. For instance, an application for #throwbackthursday has been filed by producers of an entertainment and comedy series, while #fixitjesus has been claimed by a maker of T-shirts.

As one might expect, the widespread use of hashtags has resulted in trademark disputes from time to time. In 2010, for example, a Wyoming-based chain of Mexican restaurants called Taco John's, which owns a federal registration for the mark "Taco Tuesday," sent a cease-and-desist letter to an Oklahoma restaurant called Iguana Grill, seeking to stop Iguana Grill's use of the phrase "Taco Tuesday" and the hashtag #tacotuesday for its own taco promotion. Iguana Grill did agree to stop using the name for its taco night; as of this writing, the restaurant's Facebook page exhorts customers to "Keep a look out for our taco specials . . . for *Iguana Tuesday*!" But, as is often the case with arguably heavy-handed trademark enforcement efforts, Taco John's cease-and-desist letter also resulted in considerable public criticism of Taco John's and outspoken support for Iguana Grill.

Hashtags have become ubiquitous in social media, but their status as intellectual property—particularly as trademarks—is still developing.

In March 2015, clothing maker Fraternity Collection brought trademark infringement claims in federal district court in Mississippi against a former designer based on use of the tags #fratcollection and #fraternitycollection on social media. The court accepted at the pleading stage "the notion that hashtagging a competitor's name or product in social media posts could, in certain circumstances, deceive consumers." Accordingly, the court held that Fraternity Collection's complaint stated a claim for false advertising under the Lanham Act and for trademark infringement under state law, and the court denied the designer's motion to dismiss those claims. This was, as far as we are aware, the first time that a court has found that use of a competitor's mark in a hashtag, rather than on the product itself, could result in consumer deception.

The Fraternity Collection case involved a clearly competitive use of the hashtags. What remains unclear, however, is how trademark law will treat hashtags used for non-competitive goods and services. The traditional test for infringement is the likelihood of consumer confusion. This inquiry weighs a number of factors, including the similarity of the respective marks, similarity of the respective goods or services and the advertising channels used by the parties. Thus, courts have generally found consumer confusion to be unlikely when similar or identical marks are used for unrelated goods or services that tend to be advertised in different channels. The use of identical hashtags, however, creates a single feed of all posts under the same tag, regardless of how different the advertised goods or services may be. Unlike in the physical world, where businesses can stake out non-overlapping niches for unrelated goods or services, the tag itself acts as an advertising channel on social media platforms. It remains to be seen how this functional aspect of hashtags will be weighed by the courts in the consumer confusion analysis.

As competition for attention among social media users increases, trending tags may become an increasingly prized commodity. On the other hand, given the ephemeral nature of some hashtags and the fleeting popularity of social media fads, companies should consider the long-term viability of a particular hashtag before expending time and resources to protect it. In any event, before adopting hashtags for social media campaigns, it is imperative to research potential conflicts, which may include trademark clearance searches to identify conflicting uses. And if a hashtag has already become an effective marketing tool, it may be time to consider registering it as a trademark.

SOCIAL MEDIA ASSETS IN BANKRUPTCY: FACEBOOK AND TWITTER ACCOUNTS SUBJECT TO REACH OF CREDITORS

By G. Larry Engel and Vincent J. Novak

Social media accounts can be "property of the estate" in a bankruptcy case of a business, and thus belong to the business, even when the contents of the accounts are intermingled with personal content of managers and owners. This principle was recently confirmed by the Bankruptcy Court for the Southern District of Texas in *In re CTLI, LLC* (Bankr. S.D. Tex. Apr. 3, 2015), which featured a battle among equity holders over Facebook and Twitter accounts promoting a business called Tactical Firearms.

Tactical Firearms was a gun store and shooting range. Prior to filing for bankruptcy, the business had used Facebook and Twitter accounts in its marketing. The original majority shareholder and managing office, Jeremy Alcede, had mixed his quasi-celebrity personal activities and personal politics with the promotion of the business, frequently taking to Facebook and Twitter for both personal purposes and the promotion of the business. When the company filed for bankruptcy, Alcede ultimately lost ownership and control of the company to another investor through a Chapter 11 plan of reorganization.

Despite the loss of the business, Alcede fought to retain control over the Facebook and Twitter accounts. However, although he had changed the names of the accounts to reflect his personal name rather than that of the company, the Bankruptcy Court held that the accounts belonged to the business. The court applied Bankruptcy Code § 541, which provides that a bankruptcy estate includes "all legal or equitable interests" of a debtor, in holding that the social media accounts belonged to the debtor and thus constituted property of the bankruptcy estate.

As the court recognized, Alcede had originally created the Tactical Firearms business, and the accompanying social media accounts, as "an extension of his personality" and, "like many small business owners, closely associated his own identity with that of his business." The court, however, rejected Alcede's definitions of "personal" versus "business related" media posts, finding that the best marketing for business through social media is "subtle" and can involve the use of celebrities to promote the business.

The core results of the *CTLI* decision were as follows:

1. Rejecting Alcede's property and privacy arguments, the court determined that the social media accounts were property of the bankruptcy estate, much like subscriber or customer lists, despite some intermingling with Alcede's personal social media rights. The court then exercised various remedies and contempt powers to protect the successor-owned business from Alcede's further interference and to assure that the successor could take control of the assets, including requiring delivery of possession and control of passwords for the accounts.

2. The court concluded that the "likes" that the Facebook page received belonged to the bankrupt entity, even though Alcede had registered as a Facebook user and page administrator with his personal Facebook profile. The court noted that Tactical Firearms had a Facebook page that was (a) directly linked to the Tactical Firearms web page, (b) used by Alcede and certain employees to post status updates for promoting the business, and (c) created in the name of the business rather than (until it was later improperly changed) in the name of the individual. Personal content interjected into the business page content did not change that result. Additionally, business messages to customers were communicated through the Facebook page and business-related posts.

3. The court noted that, while the business content on Tactical Firearms' Facebook page had to be accessed through Alcede's personal Facebook profile, which he had created as the registered administrator, that fact was not controlling. The business pages could be managed by multiple individuals with their profiles, and access to personal information was not necessary to manage those business pages.

4. The court also held that the Twitter account belonged to the business, given that the Twitter handle was "@tacticalfirearm" and that the account description included a description of the business.

5. The court also rejected Alcede's privacy concerns by analogizing to cases finding that parties had waived the attorney-client privilege by sharing privileged information with non-clients, or to cases where an employee used the employer's computer system and thereby waived privacy rights as to personal emails. Because the social media accounts were for the benefit of the business, Alcede lost any personal privacy right in his content and was forbidden to modify either the Facebook or Twitter account by adding or deleting any material.

Therefore, the court ordered Alcede to transfer control of the account to the new owner of the reorganized business.

The decision is noteworthy because disputes regarding social media assets, like many other rights newly created in the digital age, have generally been addressed below the public radar in bankruptcy cases and other commercial settings. This is changing, and parties in bankruptcy cases and related proceedings are increasingly focused on capturing the value of these kinds of assets.

CTLI also highlights the need to properly structure and document the various rights associated with social media accounts, as is customarily done with the intellectual property rights of inventors, authors and other creators of content or employees who are providing innovation to the businesses that employ them. The decision illustrates that equity holders and managers should discuss and plan for how to deal with their separate assets in advance of bankruptcy or other litigation.

Even if an individual wishing to preserve and shield his or her personal social media assets from related business entities has properly structured the use of the assets, a variety of other issues may arise in that individual's personal bankruptcy. In such a case, most of his or her personal social media assets would be subject to the bankruptcy and could be lost in sales for the benefit of creditors. Other social media issues that arise in bankruptcy cases of individuals are also worth considering, including the following:

- *Exempt Assets*. Only individuals (as opposed to business entities) can have personal assets that are exempt from the reach of creditors in bankruptcy. A social media account or blog and its copyrighted material could be argued to be a "tool of the trade" for a blogger and thus be exempt; however, even if that argument were to succeed (perhaps unlikely), most exemptions in bankruptcy are capped at a very low value, and the statutory exemptions are usually narrow and predate more modern classes of assets. Exemptions are thus unlikely to protect these accounts.

- *Automatic Stay*. When a bankruptcy case is filed, all acts against a debtor or its assets, including litigation against a debtor or efforts to take control of its property, are automatically stayed. However, secured lenders, who often have blanket liens on all of a borrower's assets (including social media assets), may have the ability to get relief from the automatic stay in order to foreclose on assets or pursue other remedies.

- *Rights of Publicity.* In a bankruptcy of a high-profile individual, his or her social media assets will become part of the bankruptcy estate and may be sold. However, the individual may still be able to use his or her "*persona*," or in the words of the *CTLI* court, "the interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness, and in so far as the use may be of benefit to him or others." While that "persona" interest, particularly of celebrities in states like California, has value as a type of intellectual property, there are questions as to the extent to which the assets could be marketed, particularly at the exclusion of the individual from using his or her own name and likeness in the future. Additionally, it will be inherently awkward for both the buyer and that person to compete using the same assets. Nevertheless, those assets may have strategic value to the debtor's adversaries.

As social media assets become increasingly valuable, such assets will mean more to both the owner and the owner's creditors. Valuable assets are always in play in bankruptcy cases. A bankrupt debtor may face significant challenges in starting over without the use of those social media assets in which so much was invested. These assets will increasingly be a source of disputes and will require close scrutiny.

ROLLING WITH THE PUNCHES: THE FIGHT OVER LIVESTREAMING

By Cara Ann Marr Rydbeck and Aaron P. Rubin

Boxing fans eagerly awaited the May 2, 2015, championship match between boxers Floyd Mayweather, Jr. and Manny Pacquiao. But the fight also drew the interest of those following online video apps Meerkat and Periscope. Launched at the end of February 2015, Meerkat is a livestreaming iPhone app that allows Twitter users to stream videos from their phones to their Twitter accounts in real time. The Periscope app, which Twitter acquired in January for a reported $100 million, provides similar livestreaming functionality, though Periscope's streams remain online for playback for an additional 24 hours, while Meerkat's streams can only be watched live or saved to users' individual camera rolls.

As joint producers of the Mayweather-Pacquiao fight, premium networks HBO and Showtime had exclusive rights to transmit the event live. Unless you had a ticket to the MGM Grand in Las Vegas, the only authorized way to view the fight was on pay-per-view at a cost of up to $100. Some fans, however, avoided the pay-per-view fee by watching livestreams of the event through Meerkat and Periscope. A number of Meerkat and Periscope users streamed the fight either from their seats at the arena or, more commonly, simply by pointing their phones at their television screens. Although a livestream of a TV screen may not provide great quality, it was apparently good enough for viewers to figure out what was happening in the fight. At least one stream was reported to have over 6,000 people watching at one point. Assuming a pay-per-view charge of $100 per viewer, that meant $600,000 of pay-per-view fees not being paid to HBO and Showtime.

Prior to the fight, HBO and Showtime had already taken steps to prevent piracy from eating into their pay-per-view revenues. Five days before the fight, Showtime and HBO filed a complaint in the Central District of California against nine websites that advertise that they would stream the fight for free. In the complaint, the plaintiffs, as the copyright owners of the coverage to be filmed by the single authorized camera crew, alleged direct, contributory and vicarious copyright infringement and asked for an injunction prohibiting defendants from "hosting, linking to, distributing, reproducing, performing, selling, offering for sale, making available for download, streaming or making any other use of the [c]overage." The plaintiffs also asked for damages and attorneys' fees. On April 28, 2015, the court granted plaintiffs' request for a temporary restraining order and ordered the defendants to show cause why the terms of the temporary restraining order should not be entered as a preliminary injunction.

But HBO and Showtime were unable to take similar preventive action against piracy by individual users of Meerkat and Periscope. However, after the streams began appearing, they did issue takedown requests to Periscope under the notice and takedown procedures of the Digital Millennium Copyright Act (DMCA). According to a Twitter spokesperson, Periscope, which

Sparring between content owners and users of livestreaming apps highlights the tension between the legitimate interests of content providers in preventing piracy and the equally valid interests of technology companies (and the general public) in encouraging the growth of this new technology.

operates independently of Twitter, received 66 takedown requests and took action against 30 broadcasts in response to the requests; the remaining Periscope streams had already ended or were no longer available. Compared to Periscope, Meerkat presents even greater challenges for broadcasters when it comes to policing piracy because everything on Meerkat is live, and there is no storage of streams for future viewing. As such, the policing of Meerkat streams requires real-time vigilance and action (indeed, it is unclear to what extent, if any, the DMCA's notice and takedown procedures would apply to Meerkat's current business model). According to Meerkat chief executive Ben Rubin, however, "[Meerkat] worked closely with the content owners and contacted users they alerted us about."

The Mayweather-Pacquiao fight was not HBO's first time in the ring with Periscope on piracy issues. In mid-April 2015, HBO sent takedown notices to Periscope after Periscope users livestreamed episodes of the HBO show *Game of Thrones*. Periscope reportedly took action against the infringing account holders.

All of this sparring between content owners and users of livestreaming apps highlights the tension between the legitimate interests of content providers in preventing piracy and the equally valid interests of technology companies (and the general public) in encouraging the growth of this new technology. For its part, HBO has suggested that DMCA takedown notices may not be sufficient and that app developers should "have tools which proactively prevent mass copyright infringement from occurring on their apps and not be solely reliant upon notifications." Others have opined that livestreaming apps should develop tools like Google's Content ID system, which automatically scans videos uploaded to YouTube against a database of files submitted by verified content owners and gives the owners the option of muting, blocking, monetizing or tracking the content.

It should also be noted that, depending on the circumstances and content being streamed, users of livestreaming apps may also be able to assert a fair use defense under Section 107 of the U.S. Copyright Act. For example, it would not be difficult to imagine a case similar to *Lenz v. Universal* arising in the livestreaming context. In *Lenz*, Universal Music Publishing Group objected to a YouTube video uploaded by Stephanie Lenz that showed her children dancing along to the Prince song "Let's Go Crazy." Universal issued a DMCA takedown notice to YouTube, and Ms. Lenz sent a counter-notice claiming fair use. Eventually, YouTube restored the video, and the litigation between Ms. Lenz and Universal continues to this day. The difference, of course, is that issues of fair use (and takedown notices and counter-notices) will quickly become moot in the livestreaming context due to the ephemeral nature of the medium.

Only time will tell how long and how violent the fight between content owners and users of livestreaming apps like Periscope and Meerkat will be. At least for the moment, however, it does not seem that the content owners within the mainstream entertainment industry are immune to the commercial and promotional opportunities that livestreaming apps offer. In an ironic twist, HBO itself used Periscope as part of its pre-fight hype, streaming content to its Twitter feed from Manny Pacquiao's dressing room.

EFFORT TO HIDE FACEBOOK EVIDENCE BY DEACTIVATING ACCOUNT ENDS BADLY FOR LOUISIANA MAN

By Jake Joseph Perkowski and J. Alexander Lawrence

As social media has become ubiquitous, courts are wrestling with more discovery disputes involving social media accounts.

In a recent case, *Crowe v. Marquette Transportation Co. Gulf-Inland, LLC*, the plaintiff deactivated his Facebook account in an effort to be able to claim that he was no longer on Facebook. A federal court in Louisiana rejected this ploy, ordering the plaintiff to turn over all of his Facebook data to the defendant.

Here's the background story: On May 19, 2014, Brannon Crowe sued his employer, Marquette Transportation. Crowe claimed that, in April 2014, he had an accident at work that "resulted in serious painful injuries to his knee and other parts of his body." Crowe sued for pain and suffering, medical expenses, lost wages, past and future disability, and other special damages.

But Crowe may have unwittingly shot himself in the foot (or maybe the knee). The reason? Facebook.

Around the time Crowe suffered his injuries, he sent a Facebook message to a friend saying that he had actually hurt himself while on a fishing trip.

How Marquette Transportation got its hands on the message is unclear. Nonetheless, the message led Marquette Transportation to seek other Facebook information from Crowe in discovery. On October 17, 2014, Marquette Transportation specifically requested "the Facebook history of any account(s) that [Crowe] had or has for the period commencing two (2) weeks prior to the incident in question to the present date."

Crowe objected on several grounds. First, he claimed that his account had been "hacked."

Then he suggested that the account associated with the fishing trip message was not his because the name on the account was "Brannon CroWe" and he does not capitalize the "W" in his last name.

Finally, Crowe claimed that he did not "presently have a Facebook account." When questioned about that statement in a deposition, Crowe testified that, as of October 2014, he no longer had a Facebook account. Thus, Crowe was technically telling the truth; he had deactivated his account on October 21, 2014 (four days after Crowe received the discovery request to produce his Facebook account data).

Deactivating your Facebook account, however, is not the same as deleting your account. As the Court noted, "It is readily apparent to any user who navigates to the page instructing how to deactivate an account that the two actions are different and have different consequences." Under Facebook's terms, deactivation simply means "your profile won't be visible to other people on Facebook and people won't be able to search for you," and that, upon reactivation, "[y]our profile will be restored in its entirety." In contrast, deleting your Facebook account "means you will not ever be able to reactivate or retrieve any of the content or information you've added," and there is "no option for recovery."

As to Crowe's claim that he was no longer on Facebook, the Court was having none of it. The court stated that "it is patently clear from even a cursory review that this information should have been produced as part of Crowe's original response. This production makes it plain that Crowe's testimony, at least in part, was inaccurate. That alone makes this information discoverable."

> **Deleting relevant social media data can result in sanctions because the information is not recoverable, which implicates spoliation of evidence issues.**

In short, the Court held that Crowe's Facebook-related information was discoverable because Crowe had deactivated his account to keep the evidence from his employer—and did so only after he received a discovery request.

Crowe may have inadvertently saved himself at least some trouble with the Court by deactivating his account rather than deleting it. This duty to preserve evidence in litigation extends to social media information and is triggered when a party reasonably foresees that evidence may be relevant to issues in litigation. As soon as he placed the source of his injuries at issue, Crowe triggered the duty to preserve. Deleting relevant social media data can result in sanctions against the deleting party because the information is not recoverable, which implicates spoliation of evidence issues. In contrast, Crowe's Facebook data was still accessible upon a simple re-login.

Even though Crowe did not delete his account, the Court was obviously unhappy with Crowe. The Court found that Crowe unnecessarily delayed the proceedings and wasted the Court's time by deactivating his account. And, ultimately, the Court ordered Crowe to produce all information in his Facebook account to his opponent in its entirety.

This case serves as a lesson that nothing good will come from deleting or deactivating your Facebook account to hide evidence. Even if deactivating a Facebook account to conceal damaging evidence does not constitute spoliation, because the data is ultimately recoverable, courts will inevitably come down hard on efforts to conceal evidence, even ham-handed and harebrained efforts.

THE RIGHT TO GIVE ONE-STAR REVIEWS

By Michael Wawszczak and Aaron P. Rubin

Congress has taken a step toward protecting consumers' rights to post negative reviews on websites like Ripoff Report or Yelp with the introduction, by Representative Darrell E. Issa of California, of the Consumer Review Freedom Act of 2015 (CRFA).

The CRFA follows a California law, enacted in 2014, which made it illegal for businesses to penalize their customers for posting negative reviews of their products or services online. The California law, AB 2365, was passed in response to a growing number of incidents where businesses have used non-disparagement clauses buried in form contracts to charge fines of several hundred to several thousand dollars. Such incidents have occurred all over the country—from a New York hotel withholding $500 from a couple's security deposit after a member of the couple's wedding party posted a negative review, to a Michigan-based Internet retailer charging two of its customers in Utah $3,500 after they published a review criticizing the retailer's customer service.

AB 2365 sought to put a stop to such incidents by prohibiting businesses from including in any contract for the sale or lease of consumer goods or services any provision that requires the

> **The CFRA empowers the Attorney General to bring actions for a civil penalty of up to $16,000 for each day that the business requires the use of the penalizing contract by a distinct person.**

consumer to waive his or her right "to make any statement regarding the seller or lessor or its employees or agents, or concerning the goods or services." The statute also makes it unlawful to enforce such a provision "or to otherwise penalize a consumer for making any statement protected under" the law. This is presumably intended to address situations in which a business does not explicitly prohibit negative reviews, but instead seeks to impose a penalty on a consumer who posts a negative review, as in the Michigan case noted above.

The CRFA is intended to take the California policy and expand it nationwide. Similarly to AB 2365, the CRFA prohibits businesses from including in any form contract a provision that prohibits or restricts a person from, or imposes a penalty or fee against a person for, engaging in a "written, verbal, or pictorial review, performance assessment of, or other similar analysis of, the products, services, or conduct of a business or person which is a party to the form contract." The CRFA empowers the Attorney General to bring actions for a civil penalty of up to $16,000 for each day that the business requires the use of the penalizing contract by a distinct person.

The CRFA also closes a potential loophole in AB 2365 that at least one enterprising organization had been encouraging its clients to use. Medical Justice, an organization that provides template form contracts to medical service providers, had included language in those contracts purporting to assign to the service provider the copyright in any review posted by a patient. If effective, this assignment would allow the service provider to issue takedown notices under the Digital Millennium Copyright Act or threaten the publishing websites with infringement actions. AB 2365 did not expressly address such assignment provisions, but the CRFA voids any provision that "transfers … to any person or business any intellectual property rights that the individual may have in any otherwise lawful [communication] about the person or the goods or services provided by the person or business."

Though it is unclear how likely the CRFA is to become law, it has bipartisan sponsorship, and certain key players have publicly voiced their support. For example, Yelp has come out strongly in favor of the CRFA in a post on its official blog. The bill is currently being reviewed by the House Committee on Energy and Commerce and has been referred to a subcommittee.

With a political environment that is increasingly hostile to non-disparagement clauses, businesses will now have to consider different ways of avoiding negative reviews—perhaps by providing better products and services.

THE FTC WEIGHS IN ON IN-STORE TRACKING. OR DOES IT?

By David F. McDowell, Julie O'Neill, and Adam J. Fleisher

In law school, everybody learns the adage that hard cases make bad law. When it comes to the Federal Trade Commission ("FTC" or "Commission"), a better aphorism might be, "easy cases make new law." The FTC's recent settlement with Nomi Technologies, Inc. ("Nomi") is, as the FTC's press release notes, the "FTC's first against a retail tracking company." On its face, the case is like many FTC privacy cases: it challenges a statement in the company's privacy policy for allegedly being inconsistent with the company's actual practices and thus deceptive. Under the surface, however, the case may open the door for the FTC to create a notice-and-choice regime for the physical tracking of consumers, analogous to its well-established notice-and-choice regime for online tracking.

"RETAIL TRACKING" AND NOMI'S ALLEGEDLY DECEPTIVE PRACTICES

Retail tracking occurs when retailers, or their third-party service providers, capture and track the movements of consumers in and around stores through their mobile devices, such as through the use of WiFi or beacons, in order, for example, to better understand store traffic or serve targeted offers. The FTC's Chief Technologist recently published detailed comments on the "privacy trade-offs" of retail tracking and the various technologies that companies are using to engage in it. Given the potential lack of transparency around the practice and the corresponding privacy implications, it is not surprising that the FTC decided to address the practice through its Section 5 authority, even if the FTC did so in an indirect fashion.

The facts of *In re Nomi*, as alleged in the complaint, are simple. Nomi provided mobile device tracking technology that enabled its clients, brick-and-mortar retailers, to receive analytics reports about aggregate customer traffic patterns—that is, how long consumers stay in the store and in which sections, how long they wait in line, what percentage of consumers pass by the store altogether, and so on. Nomi represented in the privacy policies posted on its website that it would "[a]lways allow consumers to opt out of Nomi's service on its website ***as well as at any retailer using Nomi's technology***." While Nomi offered an opt-out on its website, it allegedly did not provide an opt-out mechanism at its clients' retail locations, thus rendering its privacy policy promise deceptive, in violation of Section 5 of the FTC Act.

The FTC further alleged that Nomi represented, expressly or *by implication*, that consumers would be given notice when they were being tracked at a retail location. The Statement of Chairwoman Ramirez and Commissioners Brill and McSweeny in support of the complaint and proposed order explains that "the express promise of an in-store opt out necessarily makes a second, implied promise: that retailers using Nomi's service would notify consumers that the service was in use. This promise was also false. Nomi did not require its clients to provide such a notice. To our knowledge, no retailer provided such a notice on its own." By allegedly failing to provide notice when a retail location was utilizing Nomi's service to track customers, Nomi's implied promise to provide notice was also deceptive.

THE FTC KEPT NOMI NARROW. BUT REACTION HAS STILL BEEN NEGATIVE

The majority Commissioners, in their Statement, were at pains to disclaim any significance of the case with regard to the practice of retail tracking specifically:

> While the consent order does not require that Nomi provide in-store notice when a store uses its services or offer an in-store opt out, that was not the Commission's goal in bringing this case. This case is simply about ensuring that when companies promise consumers the ability to make choices, they follow through on those promises.

In spite of this effort, the FTC has received significant pushback for bringing this case in the first place, both from a member of the Commission itself and from industry groups. Industry groups such as the Application Developers Alliance have emphasized, in comments to the Commission on the proposed order, that "the inaccuracy [in Nomi's privacy policy] was de minimis and no consumer harm was alleged or apparent." These comments describe the penalty as "disproportionate" and say that "its harshness may encourage companies to simplify their data practices and privacy policies to a degree that will always ensure their legality but will also transmit very little information to the consumer," which will harm consumer choice. Comments from the U.S. Chamber of Commerce make similar points, but also note the potential of this "aggressive" enforcement of Section 5 against smaller entities to "stifle entrepreneurship and innovation in technology."

Companies that engage in in-store tracking should consider how best to provide their customers with notice and choice.

The proposed order has also come in from continued criticism from Commissioner Wright. His dissent from the vote to issue the complaint and accept the proposed consent order emphasized that the alleged misrepresentation was not material, and thus there was no deception: "Deception causes consumer harm because it influences consumer behavior—that is, the deceptive statement is one that is not merely misleading in the abstract but one that causes consumers to make choices to their detriment that they would not have otherwise made." The Commissioner continued to make his case in a recent speech to the U.S. Chamber of Commerce, emphasizing that materiality is essential to Section 5 enforcement to ensure that the Commission is actually deterring conduct that is likely to cause consumer harm and "does not chill business conduct that makes consumers better off."

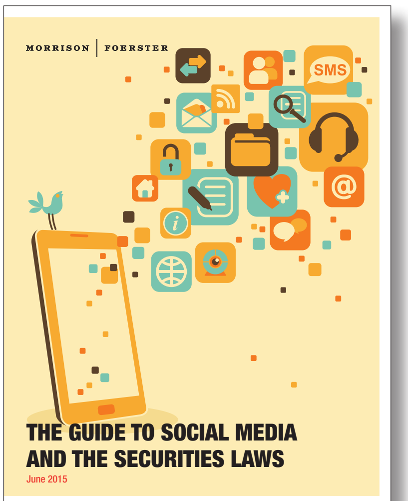
WHAT LESSONS CAN BE LEARNED?

The FTC typically moves conservatively into new areas, starting with a case that has a solid, uncontroversial grounding in established FTC precedent (such as a misrepresentation in a privacy policy). *Nomi* is the FTC's first case involving brick-and-mortar tracking, and it is highly unlikely that the FTC stumbled into a retail tracking case on accident. The Commission apparently tried to avoid controversy by providing for very narrow injunctive relief. The proposed order simply enjoins Nomi from misrepresenting how consumers can control the collection, use, disclosure or sharing of information collected from them or their devices, and from misrepresenting the extent to which consumers will receive notice about such tracking. The order itself *does not* require the company to provide notice and choice in connection with retail tracking. The Commission declined to take such a drastic step with a practice that is still, relatively speaking, in its infancy and that does not, on its face, involve sensitive personal information (though, while the information collected may be anonymous and analyzed only in aggregate, some retailers may, or at least could, pair tracking information through their apps with other information about identifying a specific consumer).

Even though the FTC has not created any new law, the pushback has still been substantial. We have no certainty around the FTC's view, but it is reasonable to anticipate that the FTC brought this case to enable it to move in a direction that mirrors its position with respect to online tracking—that is, that *at least* when information is collected for targeted advertising purposes, a company should provide meaningful disclosures to consumers about the tracking and choice with respect to whether to allow it. The FTC could ultimately deem a failure to provide such notice and/or choice an unfair and/or deceptive practice under Section 5 of the FTC Act. Whether the negative reaction to this case will slow the FTC's enforcement in this area remains to be seen.

Nevertheless, companies that engage in in-store tracking should still consider how best to provide their customers with notice and choice. Whatever the FTC does, it will probably move conservatively. That means that the FTC is likely to continue to identify practices as violations of Section 5 if they can be remedied without stifling retail tracking technology as it matures. The *Nomi* complaint presents two interrelated themes that provide a guide to future enforcement. First, choice must be linked to notice, meaning that, as far as the FTC is concerned, consumers do not have meaningful choice unless they also have notice at the point of collection, even if notice is provided only in a privacy policy only. *Nomi* can thus be read to suggest that, at least in some circumstances, choice with regard to virtual tracking needs to be accompanied by notice in the brick-and-mortar world. Second, the complaint suggests, obliquely, that tracking consumers' physical activities is "material"—i.e., that it is likely to affect consumers' conduct. If that is right, then this type of tracking must be disclosed to consumers because the failure to make such a disclosure would be, axiomatically, a material omission.

How should retailers proceed? One option is to track only those customers who have downloaded the retailer's app and affirmatively agreed to be tracked for identified purposes, such as the delivery of targeted offers. Another option is to use a vendor that subscribes to the Future of Privacy Forum Mobile Location Analytics Code of Conduct, which requires participating mobile location analytics companies to, among other things, provide consumers with appropriate notice and choice. These types of compliance strategies could help protect companies from the next possible phase of FTC enforcement in this space, since they address what appear to be, for now, the most direct ways to avoid conducting retail tracking without providing notice and choice.



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**.