Volume 7, Issue 2, March 2016

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

Sana Ayub
John F. Delaney
Adam J. Fleisher
Libby J. Greismann
J. Alexander Lawrence
Meredith W. Louis
Christine E. Lyon
Alistair Maughan
Susan McLean
Julie O'Neill
Mary Race
Anthony M. Ramirez
Joshua R. Stein
Leanne Ta
Sarah Wells

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 offer tips for a successful—and legal—advertising campaign; we examine a New York State Appellate Division opinion significantly limiting a personal-injury-case defendant's access to the plaintiff's social media posts; we review a court decision highlighting potential risks for companies seeking to exploit works licensed under the Creative Commons regime for commercial use; we take a look at an FTC report intended to help companies minimize the legal and ethical risks associated with their use of big data; we consider the complications that a federal district court opinion may create for companies hosting user-generated content; we explore the FTC's guidance for businesses that publish advertising that could be confused with editorial content; we discuss seven key things to consider when drafting the terms and conditions for a mobile app in Europe; and we describe the key provisions of the European Commission's proposed directives concerning a business's online sale of goods or digital content to consumers.

All this—plus an infographic illustrating the state of the U.S. online music industry.

INFLUENCER MARKETING: TIPS FOR A SUCCESSFUL (AND LEGAL) ADVERTISING CAMPAIGN

By Leanne Ta and Julie O'Neill

In an age of explosive growth for social media and declining TV viewership numbers, companies are partnering with so-called "influencers" to help the companies grow their brands. Popular users of Instagram, Vine, YouTube and other social media sites have gained celebrity status, generating millions of views, impressions and "likes" with every upload.

Capitalizing on the shift from traditional media to online platforms, advertisers have begun to engage influencers in marketing campaigns. In a May 2015 study, 84% of marketers said they expect to launch at least one influencer marketing campaign in the next 12 months. Of those who had already done so, 81% said influencer engagement was effective. In a separate study, 22% of marketers rated influencer marketing as the fastest-growing online customer-acquisition method.

So what is an influencer, anyway? By its broadest definition, an influencer is any person who has influence over the ideas and behaviors of others. When it comes to social media, an influencer could be someone with millions of followers or a user with just a few loyal subscribers. One thing that all influencers seem to have in common is that their audiences trust them. As such, influencers can be powerful advocates, lending credibility, increasing engagement and ultimately driving consumer actions.

Influencer marketing can be an effective tool, but it's important to do right. As recent Federal Trade Commission (FTC) and Food and Drug Administration (FDA) investigations demonstrate, online advertising is an area of relatively active enforcement, and influencer marketing presents a number of potential legal issues. The following tips can help companies lead successful influencer marketing campaigns while lessening the risk of liability.

This case raises two important questions: (1) When is a disclosure required and (2) what constitutes adequate disclosure?

DISCLOSURE IS KEY

In September, the FTC settled a case with Machinima, a company that paid popular video bloggers to promote Microsoft's Xbox One system through YouTube. Despite the hefty sums paid out to the gamers (one of whom pocketed $30,000), Machinima did not require them to make any disclosures. The FTC alleged that the failure to disclose the relationship between Machinima and the gamers was deceptive, in violation of Section 5 of the FTC Act. In its Endorsement Guides, the FTC has taken the position that a failure to disclose unexpected material connections between companies and the individuals who endorse them is deceptive.

This case raises two important questions: (1) when is a disclosure required and (2) what constitutes adequate disclosure?

Both of these questions were addressed in the FTC's comments in its 2014 investigation of Cole Haan. The investigation involved a Pinterest marketing campaign in which the company encouraged users to create boards that included five Cole Haan shoe images as well as five images of the contestants' "favorite places to wander." Contestants were instructed to use the hashtag "#WanderingSole" in each pin description. The contestant with the most creative entry would receive a $1,000 shopping spree. The FTC alleged that the contest violated Section 5 of the FTC Act for failure to disclose contestants' connection to Cole Haan.

While the FTC ultimately decided not to pursue enforcement action, the agency explained in a closing letter that entry into a contest to receive a significant prize constituted a "material connection" giving rise to a disclosure requirement. According to the FTC Endorsement Guides, a disclosure is needed whenever an endorser is given an incentive (financial or otherwise), and where knowledge of that incentive would affect the weight or credibility that audiences give to the endorser's statements or actions. Companies that work with influencers to promote the companies' brands need to make sure that audiences are aware of the relationship between the company and influencer.

As to what makes a disclosure adequate, there are, unfortunately, no magical words. The FTC Endorsement Guides state that disclosures should be clear and unambiguous; consumers should be able to find them easily and should not have to look for them. In the Cole Haan case, the FTC did not believe that the #WanderingSole hashtag adequately communicated the financial incentive between the contestants and Cole Haan. According to the Endorsement Guides, hashtags like #Promotion, #Contest or #Sweepstakes probably would have done the trick.

FIND THE RIGHT INFLUENCER

Identifying the right influencer for a marketing campaign might seem like a business decision, rather than a legal one. From a return-on-investment perspective, it's certainly important that the influencer's personality and

U.S. MUSIC CONSUMPTION

To access their favorite tunes, U.S. music fans have begun to choose streaming services over digital downloads. Here are some stats that caught our attention:

317 billion songs were streamed in 2015. That's almost double the number of songs that were streamed in 2014.[1]

965 million digital tracks were sold in 2015. That's a 12.5% decline since 2014, when 1.1 billion tracks were sold.[2]

Streaming accounted for 32% of the U.S. music industry's revenue in the first half of 2015. **Permanent downloads accounted for 40%** of that revenue.[3]

Music rights holders received $1.03 billion in revenue from streaming during the first half of 2015.[4]

Spotify, one of the most popular streaming services, **has between 25 and 30 million paid monthly listeners**, while 75 and 100 million people listen to its ad-supported free tier on a monthly basis.[5]

SOURCES

1. http://techcrunch.com/2016/01/07/nielsen-music-streams-doubled-in-2015-digital-sales-continue-to-fall/
2. http://www.billboard.com/articles/business/6835216/us-recording-industry-2015-streams-double-adele-dominates-nielsen-music
3. http://blog.discmakers.com/2016/01/music-streaming-2016-current-streaming-landscape/
4. http://blog.discmakers.com/2016/01/music-streaming-2016-current-streaming-landscape/
5. https://www.statista.com/chart/4220/music-sales-in-the-united-states/

image align with the brand, and that the influencer's audience comprises a viable customer base.

Business concerns aside, finding the "right" influencer also has legal implications. According to the FTC Endorsement Guides, "You can't talk about your experience with a product if you haven't tried it." Further, "if you were paid to try a product and you thought it was terrible, you can't say it's terrific." Thus, it's important for companies to remember that influencers must be bona fide users of the products they endorse and, if they provide a positive review, must have actually had a positive experience with those products.

THE TRUTH WILL SET YOU FREE

Influencers—and the companies they work with—can also get themselves into trouble for making false or misleading statements while endorsing a brand or product. In August 2015, the FDA took issue with an Instagram post by Kim Kardashian about a prescription drug for treating morning sickness. The post, which was sponsored by the drug manufacturer, promoted the medicine without mentioning its risks, a practice strictly forbidden by the FDA. The agency sent a warning letter alleging that post was "false or misleading in that it presents efficacy claims for [the drug], but fails to communicate any risk information associated with its use and it omits material facts." The post was taken down in response.

Companies should keep in mind that their influencers should not make any statements that their sponsoring companies can't themselves make—in other words, no false, misleading or unsubstantiated claims.

THE IMPORTANCE OF MONITORING

In recent actions, the FTC has repeatedly emphasized the importance of monitoring regimes. Cole Haan avoided enforcement action partly because it had a social media policy in place that adequately addressed issues like those described above. Likewise, Microsoft narrowly avoided being swept up in the Machinima case because Microsoft had a robust compliance program.

Ideally, companies working with influencers should have programs in place to train and monitor the influencers. It may not be enough to have the influencer sign an agreement about what he or she can and can't do. According to the Endorsement Guides, sponsoring companies must instruct influencers on their responsibilities, explain the kinds of statements they can and can't make, periodically monitor influencers' behavior and follow up if they are not playing by the rules.

KNOW YOUR INTELLECTUAL PROPERTY RIGHTS

Finally, companies should keep in mind the host of intellectual property and related issues that could arise in influencer

marketing, including trademark, copyright, privacy and publicity concerns. For example, companies may give influencers the rights to use corporate logos, branded materials or other company-owned content, but these rights should be limited to intended uses in connection with particular marketing campaigns. Further, if companies wish to own or use any influencer-generated content, those rights would ideally be documented in an assignment or license to the company.

In sum, influencer marketing can be a powerful tool, but it is important to be cognizant of potential legal concerns. Advertisers who keep these issues in mind will be in a better position to make the most of this exciting new marketing strategy.

GO FISH: DO GENERAL DISCOVERY RULES APPLY TO A LITIGANT'S FACEBOOK POSTS?

By Joshua R. Stein and J. Alexander Lawrence

Discovery of social media information has been commonplace for some time, but courts are still struggling to determine when such discovery should be allowed. While courts generally hold that normal discovery rules apply to social media discovery, at least one judge has identified—and railed against—emerging trends in such cases that impose additional hurdles for litigants seeking discovery of social media information.

Recently, in *Forman v. Henkin*, a divided New York State Appellate Division panel debated whether requests for Facebook photos are subject to the same standard that applies to any other discovery request. In this personal injury case, the plaintiff, Kelly Forman, alleged that she was injured when a leather stirrup broke while she was riding one of defendant's horses, sending her tumbling to the ground and causing Forman physical and mental injuries. Forman claimed that her injuries have limited her social and recreational activities and that her "social network went from huge to nothing."

The trial judge granted the defendant's request for Forman's social media activity, including:

(1) "all photographs of plaintiff privately posted on Facebook prior to the accident at issue that she intends to introduce at trial,"

(2) "all photographs of plaintiff privately posted on Facebook after the accident that do not show nudity or romantic encounters," and

(3) "authorizations for defendant to obtain records from Facebook showing each time plaintiff posted a private message after the accident and the number of characters or words in those messages."

In an unsigned opinion for four of the five justices on the panel, a New York appeals court reversed the trial court and substantially limited the scope of the defendant's request, allowing discovery only of photographs posted on Facebook "either before or after the accident" that Forman "intends to use at trial"—effectively gutting the discovery request.

Citing long-standing principles of discovery and New York's civil procedure rules, the panel held that discovery should include only matters "material and necessary" to the action, and that the party seeking discovery must demonstrate that the request is "reasonably calculated" to lead to relevant information. In contrast, "hypothetical speculations calculated to justify a fishing expedition" are improper.

Applying these principles, the panel concluded that the defendant failed to establish that the request for either the private photos or messages might produce relevant information.

While the legal standard for discovery may technically be clear, courts are still grappling with the level of procedural protection such information should be afforded.

While the majority resoundingly rejected the accusation that it was applying different discovery rules for social media information, Justice Saxe, dissenting, identified two emerging trends in discovery procedures that he viewed as "problematic": First, that a defendant is permitted to seek discovery of a plaintiff's nonpublic social media information "*if, and only if*, the defendant can first unearth some item from the plaintiff's publicly available social media postings that tends to conflict with or contradict the plaintiff's claims"; and second, that trial courts must then "conduct an in camera review of the materials . . . to ensure that the defendant is provided only with relevant materials." According to Justice Saxe, these two developments, applied in this case and other recent rulings, amount to extra procedural burden on the party seeking social media discovery, and add a substantial and unnecessary burden to often overworked trial courts.

Instead, Justice Saxe advocated applying the traditional discovery approach of any other document request—that is, treating social media information in the same way that any other document, tangible or electronic, is treated. Thus, a demand must have a reasoned basis that the requested category of items bears on the controversy, and must not be overbroad and fail to distinguish relevant from irrelevant items. In most contexts, the defendant describes a type of content relevant to the claimed event or injuries and the plaintiff locates such documents in his or her possession or control. Judge Saxe noted that a party is not normally required to prove the existence of relevant material before requesting it. In sum, "[u]pon receipt of an appropriately tailored demand, a plaintiff's obligation would be no different than if the demand concerned hard copies of documents in filing cabinets."

Finally, Justice Saxe pointed out that the majority's focus on "*private*" Facebook photos should not be a legitimate basis for treating social media information differently. Such "private" photos are by definition shared with at least a small universe of individuals—a Facebook user's friends or a group—and the expectation of privacy for such posts is low.

Even in light of Justice Saxe's critique, the majority held firm that the discovery standard it applied is the same for social media information as the standard that applies to any other documents and that the request was an unreasonably broad fishing expedition.

This case can perhaps best be understood as a lesson in specificity in social media discovery requests. Courts may simply feel uneasy authorizing broad discovery requests regarding social media, which they may perceive as more personal and private. The panel clearly felt uneasy about the "unbridled" scope of the social media discovery request, and suggested that the dissent's position is a slippery slope that leads to production of all information stored in "social media, a cell phone or a camera, or located in a photo album or file cabinet," or even in "diaries, letters, text messages and emails."

We wonder how the court would have dealt with a more targeted request—for instance, a request for all "private" Facebook photographs after the accident that depict Forman engaging in strenuous physical activity. As we've previously discussed, courts have regularly demanded specificity in discovery requests for social media information and have rejected requests that are not narrowly tailored to potentially relevant information.

This case demonstrates that, while the legal standard for discovery may technically be clear, courts are still grappling with the level of procedural protection such information should be afforded. This issue will surely be the topic of future litigation for years to come.

CREATIVE COMMONS WORKS: FREE TO LICENSE, BUT NOT NECESSARILY FREE TO USE

By Meredith W. Louis and John F. Delaney

Companies love to use third-party content for free. In this era of belt-tightening and slashed marketing budgets, why pay to create photos and videos for advertising and other commercial uses when compelling photos and videos are readily available online for licensing for commercial use at no charge?

Perhaps the most important source of such works is Creative Commons, a nonprofit organization that promotes the free sharing and use of copyrighted works. Creative Commons publishes user-friendly copyright licenses that are free to use, and relatively light on legalese; some of these licenses allow for even commercial use of the licensed works at no charge. Since the first Creative Commons licenses were made available in 2002, the organization estimates that hundreds of millions of works have been distributed under the Creative Commons regime, and counts Google, Wikipedia and even the White House as users.

Despite such popularity, there have been surprisingly few court decisions involving a Creative Commons license—Creative Commons identifies only nine such decisions total, and only two in the United States. A recent decision by the D.C. District Court, however, highlights potential pitfalls of the Creative Commons licensing regime for both licensors and licensees when a Creative Commons work is used for commercial purposes.

CREATIVE COMMONS LICENSING

Each of the Creative Commons license variations permits use of a copyrighted work without paying a licensing or royalty fee, provided that the licensee complies with certain conditions. The chart on page 6 summarizes the primary distinctions among the six license variations:

* Licensee must attribute the work to its author.
** Licensee may modify the work and create new works using the work.
*** Licensee must distribute derivative works under the same license terms as the original work.

THE ART DRAUGLIS DECISION

The case at hand, Art Drauglis v. Kappa Map Group, LLC, involved the commercial use of a photo on the cover of an atlas under the Attribution-ShareAlike license. While the photographer apparently did not intend his photo to be incorporated into a for-profit work, the D.C. District Court found that the disputed use fell squarely within the terms of the license.

License Type	Attribution*	Derivative Works**	ShareAlike***	Commercial Use
Attribution	Yes	Yes	No	Yes
Attribution-NoDerivs	Yes	No	No	Yes
Attribution-ShareAlike	Yes	Yes	Yes	Yes
Attribution-NonCommercial	Yes	Yes	No	No
Attribution-NonCommercial-NoDerivs	Yes	No	No	No
Attribution-NonCommercial-ShareAlike	Yes	Yes	Yes	No

The photographer, Art Drauglis, posted a landscape photograph entitled "Swain's Lock" to his public page on the photo-sharing website Flickr. Flickr offers its users the option to make their photos available for use by third parties in one of two ways: (1) By dedicating the work to the public domain (thereby waiving copyright protection), or (2) by licensing the work under a Creative Commons license (and retaining copyright in the work). Rather than selecting one of the more restrictive Creative Commons licenses, Drauglis chose the Attribution-ShareAlike 2.0 license, which allows anyone to "copy and redistribute the [licensed work] in any medium or format" and to "remix, transform, and build upon the [licensed work] for any purpose, even commercially." (Emphasis added.)

Kappa Map Group, which publishes a variety of maps and atlases, selected Swain's Lock for the cover of its 2012 "Montgomery Co., Maryland Street Atlas," which it sells for about $20. Kappa included an attribution notice on the back cover of the atlas identifying Drauglis as the photographer, as follows:

Photo: Swain's Lock, Montgomery Co., MD

Photographer: Carly Lesser & Art Drauglis, Creative Commoms [sic], CC-BY-SA-2.0

When Drauglis discovered that his photo was being used on the atlas's cover, he filed suit against Kappa, claiming that Kappa was in breach of various conditions on which the license grant was predicated and therefore was infringing his copyright.

Specifically, Drauglis argued that (1) the atlas (or at least the atlas cover) was a derivative work of his photo and, per the license's ShareAlike requirement, Kappa was obligated to distribute the atlas under similar license terms for free; (2) the photo attribution notice displayed on the atlas was insufficient because it did not include either a copy of or a URL link to the license terms; and (3) Kappa failed to comply with the license's attribution requirement because the attribution notice (which was displayed in 7-8 pt. font on the back cover) was not as prominently displayed as the copyright notice for the atlas as a whole (which was displayed in 10 pt. font on the inside cover). The court dispensed of each argument rather summarily.

Regarding Drauglis' first argument, the parties agreed (per the plain language of the license) that only "derivative works"—as distinct from "collective works"—must be distributed free of charge pursuant to the ShareAlike requirement. Indeed, the Attribution-ShareAlike license makes clear that "collective works" and "derivative works" are mutually exclusive categories – terms applying only to derivative works do not apply to collective works, and vice versa. A "collective work" is defined in the license as "a work, such as a periodical issue, anthology or encyclopedia, in which the [licensed work] in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole." Because Kappa incorporated the photo into the atlas cover "with no major deletions or alterations" and the atlas itself was a compilation of individual maps together forming a "collective whole," the court found that the atlas was a "collective work," and therefore the ShareAlike requirement did not apply.

Regarding Drauglis' second argument, the license requires that the attribution notice include "a copy of, or the Uniform Resource Identified for" the Attribution-ShareAlike license, together with information identifying the licensed work and its author(s). (Emphasis added.) Although the attribution notice used by Kappa did not include a URL link to the license terms, the court found that it did sufficiently identify them. "CC-BY-SA-2.0" is, in fact, the shorthand identifier used by Creative Commons to refer to version 2.0 of the Attribution-ShareAlike license, and the first result in a search for "CC-BY-SA-2.0" in Yahoo!, Google or Bing links directly to the license's summary page on the Creative Commons website.

Regarding Drauglis' final argument, the Attribution-ShareAlike license requires that the attribution notice

be displayed as prominently as "comparable authorship credit" appearing in a collective or derivative work. The court found that the appropriate point of comparison in this case was not the atlas copyright notice, as Drauglis argued, but rather the copyright notice for each individual map within the atlas, to which the photo attribution notice was sufficiently similar in both font size and prominence.

TAKEAWAYS

Although Drauglis' arguments were thin, and Kappa's use of the licensed photo was found to be well within the scope of the Attribution-ShareAlike license, the court nonetheless denied Kappa's request for attorneys' fees. Paying a negotiated license fee or investing in the creation of original cover art presumably would have been less costly to Kappa than 14 (long) months of discovery and litigation. Further adding to the cost of what was expected to be a fee-free license, Kappa ultimately replaced Drauglis' photo with a new cover photo (as seen here), presumably in an effort to mitigate potential damages while the trial was ongoing.

Anyone considering commercial use of a Creative Commons work should take note of this case and bear in mind the risk of litigation, as commercial uses under a Creative Commons license are seemingly more likely to be challenged by the licensee than non-commercial uses, and had Kappa not carefully complied with each applicable license requirement, the decision might well have gone the other way.

Licensors making their work available under a Creative Commons license should also take care to understand the various uses permitted under each license, rather than assuming that all Creative Commons licenses necessarily prohibit licensees from turning a profit.

BIG DATA, BIG CHALLENGES: FTC REPORT WARNS OF POTENTIAL DISCRIMINATORY EFFECTS OF BIG DATA

By Mary Race, Libby J. Greismann, Julie O'Neill and Christine E. Lyon

In a new report, the Federal Trade Commission (FTC) declines to call for new laws but makes clear that it will continue to use its existing tools it to aggressively police unfair, deceptive, or otherwise illegal uses of big data. Businesses that conduct big data analytics, or that use the results of such analysis, should familiarize themselves with the report to help ensure that their practices do not raise issues.

> A powerful tool for social good can also be used to discriminate—just as big data can enhance inclusion, it can also create exclusion.

The report, titled "Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues" grew out of a 2014 FTC workshop that brought together stakeholders to discuss big data's potential to both create opportunities for consumers and discriminate against them. The Report aims to educate businesses on key laws, and also outlines concrete steps that businesses can take to maximize the benefits of big data while avoiding potentially exclusionary or discriminatory outcomes.

WHAT IS "BIG DATA"?

The Report explains that "big data" arises from a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities of drawing connections and making inferences and predictions from collected data. The Report describes the life cycle of big data as involving four phases:

- **Collection:** Little bits of data are collected about individual consumers from a variety of sources, such as online shopping, cross-device tracking, online cookies or the Internet of Things (i.e., connected products or services).
- **Compilation and Consolidation:** The "little" data is compiled and consolidated into "big" data, often by data brokers who build profiles about individual consumers.
- **Data Mining and Analytics:** The "big" data is analyzed to uncover patterns of past consumer behavior or predict future consumer behavior.
- **Use:** Once analyzed, big data is used by companies to enhance the development of new products, individualize their marketing, and target potential consumers.

The Report focuses on the final phase of the life cycle: the use of big data. It explores how consumers may be both helped and harmed by companies' use of big data.

BENEFITS AND RISKS OF BIG DATA

The Report emphasizes that, from a policy perspective, big data can provide significant opportunities for social improvements: big data can help target educational, credit, health

care, and employment opportunities to low-income and underserved communities. For instance, the Report notes that big data is already being used to benefit underserved communities, such as by providing access to credit using nontraditional methods to establish creditworthiness, tailoring health care to individual patients' characteristics, and increasing equal access to employment to hire more diverse workforces.

On the flipside, however, a powerful tool for social good can also be used to discriminate. Just as big data can enhance inclusion, it can also create exclusion. The Report raises concerns that big data analytics may be inadvertently used to exclude certain populations, due to incomplete or inaccurate data, or hidden biases in the collection, analysis, and interpretation of the data. Data may well show correlations that are completely spurious, and if companies base marketing choices on such correlations, unintended harm to consumers may result. The Report provides the example of a credit card company lowering a customer's credit limit based not on that customer's payment history, but rather on the fact that the customer shopped at establishments where individuals with poor credit histories had also shopped. In addition, the Report expresses concern that the use of big data may assist in the targeting of vulnerable consumers for fraud, result in higher-priced goods and services for lower-income communities, and exclude such communities from certain offerings.

MAXIMIZING BENEFITS WHILE MINIMIZING RISKS

Despite recognizing the potential pitfalls of big data, the Report in no way discourages companies from using it. Rather, it seeks to help companies navigate the challenge of *how* to use big data in a way that maximizes the benefits to them and to society as a whole, while minimizing legal and ethical risks.

1. *Compliance with Potentially Applicable Laws*

Companies should understand the laws that may apply to big data practices: specifically, the Fair Credit Reporting Act (FCRA); federal equal opportunity laws, including the Equal Credit Opportunity Act (ECOA) and equal employment opportunity laws (Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act, the Fair Housing Act, and the Genetic Information Nondiscrimination Ac); and Section 5 of the FTC Act.

- ***The FCRA*** imposes obligations on companies that compile, sell, or use consumer reports. Recent FTC enforcement actions, including *United States v. Spokeo, Inc.*, and *United States v. Instant Checkmate, Inc.*, demonstrate that the FCRA extends beyond traditional credit bureaus to data brokers that compile nontraditional information, including social media information, if that information is used for consumer eligibility decisions. If a company uses big data products to make eligibility decisions (such as to determine a consumer's eligibility for credit, employment, insurance, or housing), it should make sure that it has complied with all applicable FCRA requirements, including certifying that it has a permissible purpose for obtaining the information and that it will not use the information to violate equal opportunity laws. Similarly, the company must provide consumers with any notices required under the FCRA (such as notice of adverse action taken based on information in a consumer report) and obtain any required authorizations (such as to procure a consumer report for employment purposes).

- ***Federal equal opportunity laws*** prohibit discrimination based on protected characteristics such as race, color, sex, religion, age, disability, national origin, marital status, and genetic information. Discrimination may take the form of disparate treatment (intentionally treating an individual differently based on a protected characteristic) or disparate impact (applying a facially neutral policy that has a disproportionate adverse effect on individuals with a protected characteristic). The Report suggests, for example, that it may be problematic under the ECOA for a company to make credit decisions based on consumers' zip codes, if the decisions have a disproportionate adverse impact on a particular ethnic group and are not justified by a legitimate business necessity. Companies should thus examine whether their use of big data results in the treatment of people differently on a prohibited basis, whether directly or indirectly, and take steps to remedy any such discrepancies.

- ***Section 5 of the FTC Act*** prohibits unfair or deceptive acts or practices. Companies engaging in big data analytics should consider whether they are violating any material promises to consumers, such as a promise to refrain from sharing consumer data or an assurance that they will safeguard it. Further, companies that supply big data to other companies should undertake reasonable measures to know the purposes for which their customers will use the data. For example, companies should take steps to ensure that their customers will not use big data to commit fraud or for discriminatory purposes.

The Report urges companies to proceed with caution when using big data in ways that could lead them to violate these and other potentially applicable laws.

2. *Policy Considerations for Big Data Research*

The Report urges companies to take into account the special policy considerations raised by big data

research. To help minimize the potential for discriminatory harm arising out of such research, the Report encourages companies to address the following questions:

- **How representative are your data sets?** Consider whether your data sets are missing information from particular populations and, if so, take steps to address issues of under- and overrepresentation.

- **Does your data model account for biases?** Review your data sets and algorithms to ensure that hidden biases do not have an unintended impact on certain populations.

- **How accurate are your predictions based on big data?** Remember that just because your big data analytics found a correlation, the correlation is not necessarily meaningful. Human oversight of big data tools may be worthwhile, particularly when decisions implicating health care, credit, or employment are involved.

- **Does your reliance on big data raise ethical or fairness concerns?** Consider whether such concerns advise against using big data in certain circumstances. Consider further whether you can use big data to advance opportunities for underserved populations.

CONCLUSION

Particularly in light of ever-developing technologies, big data will certainly continue to grow in importance. The Report makes clear that the FTC will continue to monitor companies' legal obligations around its use. Accordingly, companies should carefully examine their big data practices to identify and take steps to help minimize the risks they may present.

NEW COURT DECISION HIGHLIGHTS POTENTIAL HEADACHE FOR COMPANIES HOSTING USER-GENERATED CONTENT

By Anthony M. Ramirez and John F. Delaney

In this election season, we hear a lot of complaints about laws stifling business innovation. And there is no doubt that some laws have this effect.

But what about laws that spur innovation, that result in the creation of revolutionary new business models?

Section 512(c) of the Digital Millennium Copyright Act (the DMCA) is one such law. Passed by Congress and signed by President Bill Clinton in 1998, Section 512(c) has played an enormous role in the success of YouTube, Facebook and other social media platforms that host user-generated content, by shielding such platforms from monetary damages from copyright infringement claims in connection with such content.

Absent this safe harbor, it is difficult to imagine a company like YouTube thriving as a business. For example, in 2014 alone, YouTube removed over 180 million videos from its platform due to "policy violations," the vast majority of which likely stemmed from alleged copyright infringement; yet, absent the Section 512(c) safe harbor, YouTube could have been exposed to staggering monetary damages in connection with those videos.

The DMCA's protection from liability is expansive, but it is not automatic. To qualify, online service providers must affirmatively comply with a number of requirements imposed by the law. While most of those requirements may seem straightforward, a recent case in the Southern District of New York illustrates how even seemingly routine paperwork can pose problems for websites that host user-generated content.

For companies seeking protection under the DMCA, the typical starting point is designating an agent to receive "takedown" notices from copyright owners. If a company is sued for copyright infringement relating to user-generated content on its website, that company will want to show that it has designated a DMCA agent. But what if the designation paperwork was handled by another entity within the defendant's organizational structure, such as a corporate parent? That was the situation faced by one of the defendants in *BWP Media USA Inc., et al. v. Hollywood Fan Sites LLC, et al.* (S.D.N.Y. 2015)—and the court held that the defendant was out of luck.

> Absent the Section 512(c) safe harbor, it is difficult to imagine a company like YouTube thriving as a business.

Although the defendant's corporate parent had filed a registration form with the U.S. Copyright Office under the parent's name, nothing on the form mentioned the defendant or made any general reference to affiliates. Under those circumstances, the court concluded that the defendant was ineligible for the safe harbor because it had "no presence at all" in the Copyright Office's directory of DMCA agents. The court reasoned that those searching the Copyright Office directory should not be "expected to have independent knowledge of the corporate structure of a particular service provider."

Despite lacking a Copyright Office registration, the defendant argued that it did actually post the agent's information on its own website, and that one of the plaintiffs had successfully used such information to send a takedown notice resulting in removal of the allegedly infringing material. The court found those assertions "irrelevant," because they did nothing to address the Copyright Office registration requirement. As the court noted, the DMCA requires each service provider to post the agent's name and contact information on the provider's website, *and* submit such information to the Copyright Office.

Would the defendant's DMCA eligibility have turned out differently if the parent had included the affiliate's name on the form, or at least made a general reference to the existence of affiliates? The court's opinion leaves those questions unaddressed, but the preamble to the Copyright Office regulations—cited in passing by the court—appears to reject such an approach. According to the preamble, each designation "may be filed only on behalf of a single service provider[, and] related companies (e.g., parents and subsidiaries) are considered separate service providers who would file separate [designations]."

Following the *Hollywood Fan Sites* decision, we expect that many companies that host user-generated content will be checking to make sure that all of their legal names are indeed listed in the Copyright Office directory—and, in light of the Copyright Office's position on this subject, many such companies may also decide to file separate designations for each legal entity within a corporate family. While this process may be cumbersome, it seems a small price to pay for the generous safe harbor benefits offered by the DMCA, especially for companies with business models that depend on user-generated content.

AN FTC WARNING ON NATIVE ADVERTISING

By Julie O'Neill and Adam Fleisher

"Native advertising"—ads that may blur the distinction between advertising and editorial, video or other content—has been a hot topic in recent years for both marketers and regulators. It is popular with marketers because it is apparently an effective advertising model. The Federal Trade Commission (FTC), on the other hand, contends that it may be deceptive when the advertising content is not readily identifiable to consumers as such, and it has just issued guidance on how advertisers can stay on the right side of the law. On December 22, 2015, the FTC released an Enforcement Policy Statement on Deceptively Formatted Advertisements that focuses in particular on "native" advertising, along with guidance for businesses on native advertising that further fleshes out the FTC's expectations.

The FTC may deem an ad that looks like an ordinary news article to be deceptive if consumers are not provided with sufficient information to differentiate the ad from publisher-generated, non-advertising content.

The Enforcement Policy Statement defines "natively formatted advertising" as communications "that match the design, style, and behavior of the digital media in which it is disseminated." For example, an advertisement may be integrated into a newspaper website, with a "headline" and then a few lines of text, so that it appears similar to substantive, publisher-generated news articles posted on the website. Native advertisements may also appear on social media platforms and may be delivered as videos or through other media.

Regardless of format, the rule is the same. As the Statement puts it:

Deception occurs when an advertisement misleads reasonable consumers as to its true nature or source, including that a party other than the sponsoring advertiser is the source of an advertising or promotional message, and such misleading representation is material.

In light of this principle, the FTC may deem an advertisement that looks like an ordinary news article to be deceptive if consumers are not provided with sufficient information to differentiate the advertisement from publisher-generated, non-advertising content. This information may be inherent in the nature of the advertisement, or it may require a separate disclosure indicating that the advertisement is a marketing communication. For example, in *FTC v. Coulomb Media, Inc.*, as well as other cases, the FTC alleged that defendants deceptively used fake news websites to market açai berry products. Similarly, and more recently, in *FTC v. NourishLife, LLC*, the FTC alleged that the defendants misrepresented that a so-called research website was an independent source for information about the speech disorder apraxia, when in fact the website advertised the health benefits of the company's products.

A disclosure may be important because, even if the substance of the natively formatted advertisement is not deceptive, the *nature of the advertisement itself* can be deceptive. In this regard, the FTC has recently brought enforcement actions and warned about advertising that appears to be user-generated commentary about a product or service but is in fact marketing content created by or on behalf of an

advertiser. You can read more about these enforcement actions here and here.

To put it another way, the Enforcement Policy Statement holds that "an ad is deceptive if it promotes the benefits and attributes of goods and services, but is not readily identifiable to consumers as an ad." But what, exactly, does that mean? The Policy Statement and the guide for businesses offer some considerations of what may make an advertisement "readily identifiable." The guidance lists 17 mini case studies that provide examples of what does and does not require a disclosure. (The fact that 17 examples are necessary suggests the potential complexity in making this determination.) The recurring theme of the examples is whether the consumer can reasonably ascertain that the advertisement is paid marketing material and not content organically generated by the publisher (or by a user in the case of social media or video-hosting websites).

For cases in which native advertising requires a disclosure, the new guidance recaps the FTC's *.com Disclosures* guidance for businesses, which lays out basic requirements for making "clear and prominent" disclosures. The guidance also adds some new considerations, such as the need to disclose that the native content is advertising near the focal point of the ad, or in front of or above the "headline" of the native advertisement. (This disclosure needs to convey to the consumer that the material is advertising *before* the consumer clicks through the ad to the main advertising page.) In addition, the guidance suggests that, for multimedia ads (such as videos), the disclosure should be made in the video itself *before the consumer receives the advertising message*. That is, if the advertisement is only a small part of the overall video, the disclosure must be "delivered as close as possible to the advertising messag[e]" itself. Finally, the guidance affirms that the disclosures should include terms likely to be understood, such as "Ad," "Advertisement," or "Paid Advertisement," and *not* terms such as "Promoted" or "Sponsored," which are ambiguous in this context and could imply, for example, that a sponsoring advertiser funded the content but did not create or influence it.

As the FTC continues to scrutinize various mechanisms for delivering advertising online, companies should make sure that consumers are aware when they are being marketed to, even as the participants in the digital advertising ecosystem come up with new and innovative ways to deliver those marketing messages. All participants, including the companies whose products are being marketed, are potentially at risk of an FTC enforcement action if their advertisements are found to be deceptive, and thus every participant should pay heed to the FTC's recent statements and guidance. In light of the FTC's aggressive approach in this area, making sure that innovative forms of advertising meet the FTC's timeless disclosure standards should be on every company's radar.

LAUNCHING A MOBILE APP IN EUROPE? SEVEN THINGS TO CONSIDER WHEN DRAFTING THE TERMS & CONDITIONS

By Susan McLean and Sarah Wells

[Editor's Note: In response to the success of our earlier post on terms and conditions for mobile apps, two of our London-based colleagues have prepared a "remixed" version, which looks at the subject of mobile app terms and conditions from a European perspective. Enjoy!]

The mobile app has become the new face of business. It's no longer sufficient to have a company website. More and more companies want a mobile app that users can download to their smartphones and easily access. It's not difficult to see why. People are voting with their thumbs.

One of the key legal protections your company will need in connection with such launch is an end user license agreement.

In 2015, overall mobile app usage grew by 58%, with lifestyle and shopping apps growing 81%, following previous 174% growth in 2014, according to FlurryMobile. Indeed, FlurryMobile figures show that mobile commerce now accounts for 40% of online commerce worldwide. Accordingly, the advantages of an app to business, from a customer marketing, engagement, service and awareness perspective, are clear.

Even traditionally conservative sectors such as financial services are being revolutionised by the mobile app. In 2015, the British Bankers Association identified that banking by smartphone and tablet has become the main way for UK customers to manage their finances, with mobile banking overtaking branches and the internet as the most popular way to bank.

If your company will be among the many businesses that launch a mobile app in Europe in 2016, one of the key legal protections your company will need in connection with such launch is an end user licence agreement (EULA). So, where do you start? Here at MoFo, we regularly review mobile app EULAs and we've noticed a number of issues that app developers don't always get right. Here is our list of the key issues you will need to consider.

1. *One size does not fit all*

Your EULA will be an important part of your strategy to help mitigate risks and protect your intellectual property in connection with your app. It's unlikely that you would release desktop software without an EULA, and mobile apps (which are, after all, software products) warrant the same protection. While platforms such as 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 customized EULAs instead—subject to a few caveats, as mentioned below. Because the default EULAs can be quite limited and can't possibly address all of the issues that your particular app is likely to raise, it's generally best to adopt your own EULA in order to protect your interests.

2. *How to ensure a binding EULA?*

Whether an EULA is enforceable in any particular case will depend on how the EULA is presented to users and how users indicate their agreement to the EULA. There are several ways that you can present your EULAs to users. For example, in most app stores, a dedicated link called "Licence Agreement allows companies to include a link to their EULAs from their product page. In addition, it's advisable for companies to include language in their apps' "Description" field making clear to users that, by downloading and using the app, they are accepting the EULA. Despite this functionality being available, many apps currently do not provide users with an opportunity to view the EULA before downloading the app. However, if you want to help ensure your EULA is capable of being enforced against consumers in Europe, the safest approach is to include a link to the EULA and require an affirmative "click-accept" of the EULA when the app is first opened by a user on his or her device to demonstrate that the EULA was accepted.

3. *Who is bound by your EULA?*

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. If minors will be permitted to use the app, then the EULA should require that a parent or guardian consents on the minor's behalf. If the app is specifically targeted at minors, careful consideration should be given to any specific legal or regulatory requirements. For example, in Europe, particular concerns have been raised about the use of app games by minors, particularly games that are free to download, but which provide for in-app purchases; regulators have issued specific guidance of which developers of app games will need to be aware.

4. *Where to put your EULA?*

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 first 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, with the second 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 the associated risk issues. We note that, under applicable consumer law in Europe, any EULA term that has the object or effect of enabling the developer to alter the terms of the contract unilaterally without a valid reason is likely to be considered unfair.

5. *What about app store terms?*

Some app stores understandably require that, if a company adopts a customized EULA for its app, that 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 apply.) Other third-party terms may also apply, depending on any third-party functionalities or opensource 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. *Consumer protection*

There are various consumer protection requirements that will need to be considered if your app is going to be targeted at consumers in Europe. In particular, specific information will need to be provided to such consumers, including with respect to the identity of the app developer, app charges, functionality of the app, how the app operates with relevant hardware/software (interoperability), and whether any geographical restrictions apply, and so forth. Consumers also have a right to withdraw from the contract, *i.e.* "return" the app within 14 days of concluding the contract, except where the consumer expressly consents to the download and acknowledges that in completing the download the user will lose this cancellation right. Therefore, it's important in Europe for your EULA to contain an acknowledgment that the consumer waives this cancellation right on download of the app.

In addition, within Europe, individual member states may have other requirements affecting apps that you will

need to take into account. Although most EU member states don't currently have national consumer protection legislation specifically concerning sales of digital content to consumers, since October 1, 2015, UK consumers have enjoyed new rights and remedies with respect to digital content. Any company targeting an app at consumers in the UK should now take into account implied quality standards in terms of satisfactory quality, fitness for purpose and compliance with description. Also, even where the app is provided free of charge, if the app causes damage to a consumer's device or other digital content, then the app provider will be liable for such damage. As detailed in our post on This lack of harmonisation within Europe has led to the European Commission proposing new EU laws that would give consumers new rights of remedy and redress where digital content is faulty or inadequately described by the seller.

7. Be clear and fair

It's not just a question of what information to include in your EULA, it's also important to carefully consider how your EULA is written. A common complaint is that EULAs are too long, filled with impenetrable jargon and hard to read, created more to protect companies in the court room than help the consumer make an informed choice.

In order to avoid the wrath of European consumer protection regulators, and to help ensure that your EULA is enforceable, you should aim to use plain language that is understandable to consumers. Where complex and technical issues need to be covered, particular care will be needed. You should avoid obscure legal jargon, including removing references to phrases which may be unfamiliar to consumers such as "indemnities", "consequential loss", "assignment", etc. In addition, because space on a mobile device screen is limited, it's advisable to keep the terms as concise as possible and easy to navigate.

Even if a EULA is written in plain language, extremely one-sided provisions—such as a disclaimer of direct damages (rather than a cap on such damages)—are at risk of being held to be unfair and unenforceable against the consumer. At the same time, the EULA is ultimately a legal document, and so you'll want to make sure that any slimmed-down or simplified EULA still provides you with adequate protection.

Of course, it's not just a question of compliance with consumer law. Where your app relates to a regulated sector, *e.g.* financial services, health and gambling, there are likely to be other regulatory requirements that you will need to comply with. And these regulatory requirements may go beyond the EULA itself and affect the way the app is designed and structured. Therefore, it's very important to consider compliance issues from the development stage.

Lastly, if you collect personal information through your mobile app, remember that, in addition to your EULA, you will need to have a privacy policy in place and ensure that you comply with applicable data protection and privacy laws; such laws are often far more burdensome in Europe than in the United States—but that's a topic for a separate article!

HARMONIZING B2C ONLINE SALES OF GOODS AND DIGITAL CONTENT IN EUROPE

By Alistair Maughan and Sana Ayub

The European Commission has announced new draft laws that would give consumers new remedies where digital content supplied online is defective or not as described by the seller.

On Dec. 9, 2015, the European Commission proposed two new directives on the supply of digital content and the online sale of goods. In doing so, the Commission is making progress towards one of the main goals in the Digital Single Market Strategy (the "DSM Strategy") announced in May 2015: to strengthen the European digital economy and increase consumer confidence in trading across EU Member States.

This is not the first time that the Commission has tried to align consumer laws across the EU; its last attempt at a Common European Sales Law faltered earlier this year. But the Commission has now proposed two new directives, dealing both with contracts for the supply of digital content and other online sales (the "Proposed Directives").

The issue with previous EU legislative initiatives is that "harmonized" has really meant "the same as long as a country doesn't want to do anything different."

National parliaments can raise objections to the Proposed Directives within eight weeks, on the grounds of non-compliance with the subsidiarity principle—that is, by arguing that that regulation of digital content and online sales is more effectively dealt with at a national level.

Objectives

Part of the issue with previous EU legislative initiatives in this area is that "harmonized" has really meant "the same as long as a country doesn't want to do anything different." This time, the Proposed Directives have been drafted as so-called "maximum harmonization measures," which would preclude Member States from providing any greater or lesser protection on the matters falling within their scope. The

Commission hopes that this consistent approach across Member States will encourage consumers to enter into transactions across EU borders, while also allowing traders to simplify their legal documentation by using a single set of terms and conditions for all customers within the EU.

An outline of the scope and key provisions of each of the Proposed Directives, as well as the effect on English law, are summarized after the jump.

DRAFT DIGITAL CONTENT DIRECTIVE

Scope

The draft digital content directive would apply only in business-to-consumer sales, and would not extend to small and medium-sized enterprises—nor to digital content providers in certain sectors such as financial services, gambling or healthcare. The rules would apply regardless of the method of sale, unlike the draft online goods directive. The directive would cover consumers who provide non-monetary consideration in exchange for digital content, such as personal data.

Key Provisions

- Digital content would now expressly include cloud computing and use of social media, and would attract quality standards and statutory remedies for consumers.

- Digital content will be required to conform to key information provided to consumers, such as quality, interoperability, accessibility and security. If content does not conform, the consumer will have rights to require the provider to make it conform, or to receive a refund or terminate the contract.

- Under present English law, the Consumer Rights Act 2015 ("CRA") applies only where digital content has been paid for. The draft digital content directive would extend the scope of consumer rights to cases where the buyer provides non-monetary consideration such as personal data, thus providing greater protection to consumers than is currently being offered under the CRA. On any termination, businesses would be prohibited from making further use of non-monetary consideration provided by consumers.

- Digital content would need to be provided instantly and in its most recent version, unless otherwise agreed. Where the content is not provided instantly or at its agreed time, the consumer would have a right to terminate immediately.

- The draft digital content directive would remove the current 6-month time limit under the CRA for the presumption that defects are present on delivery (unless the consumer had been forewarned that the digital content was incompatible with the consumer's digital environment).

- Consumers will have the right to terminate a contract under which digital content is provided on an ongoing basis, if the business modifies the contract to the detriment of the consumer. Furthermore, the business would be required to give notice of the actual changes, and would only be entitled to implement those changes if the contract permitted it.

DRAFT ONLINE GOODS DIRECTIVE

Scope

As with the draft digital content directive, the draft online goods directive would only apply in business-to-consumer sales. Only goods sold online or otherwise at a distance fall within scope. As such, any face-to-face sales are not covered. Contracts for the supply of services would not be subject to this directive. Where a contract is for the supply of both goods and services, the rules would apply only to those elements of the contract that relate to the goods.

Key Provisions

- Consumers would no longer have a right to reject goods unless a repair or replacement had first been requested and been deemed unsuccessful.

- Emerging defects that are presumed to be present on delivery currently have a time limit of six months under the CRA. The draft online goods directive would extend this to two years.

- In the context of known defects, traders would be required to obtain express consent from consumers in order to escape liability. It will no longer be sufficient to rely on such defects being obvious, or being brought to the customer's attention.

While some Member States have expressed concerns regarding the practicalities of having separate rules for online and offline sales, there does appear to be support for action at the EU-level regarding digital content. If the Proposed Directives are successfully adopted in accordance with the ordinary legislative procedure, the Commission will finally be putting its push for harmonization into practice.

SXSW 2016

We're looking forward to attending SXSW Interactive, March 11-16, 2016. Please let us know if you will be there.

We would love to connect with you in Austin!

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**.

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, and technology and life sciences companies. The *Financial Times* has named the firm to its lists of most innovative law firms in Northern America and Asia every year that it has published its Innovative Lawyers Reports in those regions. In the past few years, *Chambers USA* has honored MoFo's Bankruptcy and IP teams with Firm of the Year awards, the Corporate/M&A team with a client service award, and the firm as a whole as Global USA Firm of the Year. Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger.